KENYA PIPELINE COMPANY PLC

KENPIPE PLAZA, SEKONDI ROAD,
OFF NANYUKI ROAD, INDUSTRIAL AREA
P.O. BOX 73442-00100
NAIROBI
Website : www.kpc.co.ke

RE- TENDER

TENDER FOR DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF

AN

ENTERPRISE DIGITAL SOLUTION

TENDER REFERENCE: *KPC/PU/OT/134/ICT/NBI/26-27*

November 2026

IMPORTANT NOTICE TO TENDERERS

This Standard Tender Document (STD) is issued by Kenya Pipeline Company PLC (KPC PLC) for the procurement of Information Technology projects encompassing hardware, software, licences, implementation services, support, maintenance and related IT services. It is a master document to be read with the Data Sheet, Technical Specifications/Terms of Reference and Project Charter for each specific procurement.

WHERE THERE IS CONFLICT between this ITT and the Data Sheet or Technical Specifications/Terms of Reference, the Data Sheet and Technical Specifications/Terms of Reference shall prevail.

Digital-First Procurement: KPC PLC conducts all procurement through its secure SAP SRM e-procurement portal. The portal enforces all tendering rules digitally, including separation of technical and financial proposals, simultaneous proposal opening, automatic enforcement of technical qualification thresholds before financial evaluation, and structured scoring. Physical submission is a limited exception for exceptional circumstances only as specified in the Data Sheet.

This STD generally applies to the following IT procurement categories:

- Hardware: Servers, storage, networking equipment, end-user devices (laptops, desktops, tablets), printers, peripherals, UPS, data centre equipment, industrial IoT/SCADA hardware
- Software: Enterprise applications (ERP, CRM, HRMS, EAM), industry-specific systems (SCADA, Accuload, pipeline management, metering, etc), productivity software, operating systems, databases, middleware
- Licences: Software licences (perpetual, subscription, concurrent, site-wide), cloud platform licences, SaaS subscriptions, API access licences
- Implementation Services: System design, configuration, customisation, data migration, integration, testing, training, go-live support, documentation
- Support and Maintenance: Annual maintenance contracts (AMC), service level agreements (SLA), helpdesk services, patch management, software updates/upgrades, break-fix support
- Managed Services: IT infrastructure managed services, cloud managed services, cybersecurity managed detection and response (MDR), network operations centre (NOC) services
- IT Consultancy within IT Projects: Technical advisory, project management, architecture design, cybersecurity assessment — as a component of a larger IT project

However, the above does not constitute the scope of thus procurement. The same is outlined in the Terms of Reference.

Table of Contents

IMPORTANT NOTICE TO TENDERERS 2
SECTION I: INSTRUCTIONS TO TENDERERS (ITT) 10
A. GENERAL 10
1. Scope of Tender 10
2. Definitions 10
3. Eligible Tenderers 11
4. Conflict of Interest 11
5. Corrupt and Fraudulent Practices 12
B. PREPARATION OF TENDERS 12
6. Cost of Tendering 12
7. Language 12
8. Documents Comprising the Tender 12
9. Lots and Multi-Component Proposals 13
10. Tender Validity and Prices 13
11. Tender Security 13
12. Clarifications and Pre-Tender Meeting 13
C. SUBMISSION — DIGITAL-FIRST APPROACH 13
13. Primary Submission: SAP SRM Portal 13
14. Physical Submission — Exception Only 14
15. Submission Deadline and Late Tenders 14
16. Opening of Tenders 14
D. EVALUATION AND AWARD 15
17. Evaluation Process Overview 15
18. Negotiations 15
19. Award, Notification and Contract Signing 15
E. COMPLAINTS 15
20. Complaint Mechanism 15
SECTION II: TENDER DATA SHEET (TDS) 17
SECTION II-A: TERMS OF REFERENCE 22
1.0 Introduction of KPC 22
1.0.1 Core Business Functions 22
1.0.2 Business Model 23
1.0.3 Organizational Structure and Business Units 23
1.0.4 Geographical Coverage 24
1.0.5 Workforce 24

1.0.6 Key Stakeholders....25
1.0.7 Current Systems and Enterprise Technology Landscape....25
1.0.8 Enterprise Systems Landscape....26
1.0.9 Operational Technology (OT) Landscape....28
1.0.10 Integration Landscape....28
1.0.11 Data, Reporting, and Analytics....30
1.0.12 Customization Landscape....30
1.0.13 Infrastructure Landscape....31
1.0.14 Current Challenges....32
2.0 Digital Transformation Project....32
2.0.1 Project Overview....33
2.0.2 Roles and Responsibilities....33
2.0.3 Desired Architecture....36
LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES....37
2.1.1 Objectives of LOT 1....37
2.1.2 Scope of Services....38
2.1.3 Programme Lifecycle Support....39
2.1.4 Key Deliverables....40
2.1.5 Programme Governance Framework....41
2.1.6 Staffing and Key Personnel Requirements....45
2.1.7 Deliverables and Reporting Requirements....48
2.1.8 Service Levels and Key Performance Indicators (KPIs)....52
2.1.9 Acceptance Criteria....55
2.1.10 Performance-Based Payment Milestones....57
LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION....60
2.2.1 Introduction....60
2.2.2 Objectives of LOT 2....60
2.2.3 Scope of the Enterprise Digital Transformation Solution....61
2.2.4 Specifications....80
2.2.5 Implementation Services....251
2.2.6 Bill of Materials (BOM)....292
2.2.7 Additional Information to the Scope and Requirements....336
SECTION III: TENDER SUBMISSION FORMS....341
FORM TP-IT-1A: TECHNICAL PROPOSAL SUBMISSION FORM....341
FORM TP-IT-2A: TENDERER PROFILE AND CORPORATE CREDENTIALS....343
FORM TP-IT-2B: TENDERERS RELEVANT EXPERIENCE....344

FORM TP-IT-3: TECHNICAL SOLUTION DESCRIPTION – For LOT 2 Only 347
FORM TP-IT-4: TECHNICAL COMPLIANCE MATRIX – LOT 2 Only 349
FORM TP-IT-5A: PROJECT MANAGEMENT METHODOLOGY – LOT 1 350
FORM TP-IT-5B: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN – LOT 2 351
FORM TP-IT-6: PROPOSED TEAM — KEY PERSONNEL 352
FORM TP-IT-7: AFTER-SALES SUPPORT AND SERVICE LEVEL AGREEMENT PROPOSAL 353
FORM TP-IT-8A PART 1: CYBERSECURITY AND DATA PROTECTION DECLARATION354
FORM TP-IT-8 PART 2: CYBERSECURITY AND DATA PROTECTION DECLARATION . 354
FORM TP-IT-9: TECHNICAL BILL OF MATERIAL 355
LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES 355
LOT 2: DESIGN, SUPPLY, IMPLEMENATION, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL TRANSFORMATION SOLUTION 355
FORM OEM-IT: OEM AUTHORISATION LETTERS – Required for Lot 2: Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution Only 381
FORM COI-IT: CONFLICT OF INTEREST DECLARATION 382
FORM BOD-IT: BENEFICIAL OWNERSHIP DISCLOSURE 382
FORM ACD-IT: ANTI-CORRUPTION DECLARATION 383
FINANCIAL PROPOSAL FORMS — SUBMIT SEPARATELY IN SAP SRM PORTAL 383
FORM FP-IT-1: FINANCIAL PROPOSAL SUBMISSION FORM 383
FORM FP-IT-2: BILL OF MATERIALS AND TOTAL COST SCHEDULE 384
FORM FP-IT-2A: LOT 1 – PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES – BILL OF MATERIALS / PRICING SCHEDULE 384
FORM FP-IT-2B: LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION – BILL OF MATERIALS 385
SECTION IV: IT PROCUREMENT EVALUATION FRAMEWORK 415
B. STAGE 1 — PRELIMINARY / ADMINISTRATIVE REVIEW (PASS/FAIL) 415
C. STAGE 2 — TECHNICAL COMPLIANCE REVIEW (PASS/FAIL) 416
LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES 416
LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION 419
D. STAGE 3 — TECHNICAL SCORING 425
E. STAGE 3B — SCRIPTED DEMONSTRATION (LOT 2, PASS/FAIL) 432
F. STAGE 5 — FINANCIAL AND TCO EVALUATION 433
F.1 Financial Proposal Completeness Review 433
F.2 Total Cost of Ownership (TCO) Calculation – LOT 2 Only 433

F.3 Financial Scoring 434
G. COMBINED SCORING AND AWARD RECOMMENDATION 434
Final Evaluation – Award Criteria 434
Quality and Cost Based Selection (QCBS) 434
H. POST-QUALIFICATION VERIFICATION 435
SECTION V: GENERAL CONDITIONS OF CONTRACT FOR IT PROCUREMENT (GCC-IT) 437
1. DEFINITIONS 437
2. APPLICABLE LAW AND JURISDICTION 438
3. CONTRACT DOCUMENTS AND PRIORITY 438
4. SCOPE OF SUPPLY AND SERVICES 438
5. HARDWARE SUPPLY 439
6. SOFTWARE AND LICENCES 439
7. SOFTWARE ESCROW 440
8. DELIVERY, INSTALLATION AND COMMISSIONING 440
9. ACCEPTANCE 440
10. PROJECT MANAGEMENT 441
11. CHANGE MANAGEMENT 441
12. WARRANTY 441
13. SERVICE LEVEL AGREEMENT (SLA) 442
14. CYBERSECURITY OBLIGATIONS 442
15. DATA PROTECTION 443
16. INTELLECTUAL PROPERTY 443
17. PAYMENT 444
18. LIQUIDATED DAMAGES 444
19. PERFORMANCE SECURITY 444
20. AUDIT RIGHTS 445
21. CONFIDENTIALITY 445
22. FORCE MAJEURE 446
23. SUSPENSION 446
24. TERMINATION 446
25. TRANSITION AND EXIT 446
26. LIMITATION OF LIABILITY 447
27. DISPUTE RESOLUTION 447
28. NON-SOLICITATION 447
29. NON-WAIVER AND SEVERABILITY 447
30. NOTICES 448

31. ENTIRE AGREEMENT 448
SECTION VI-A: SPECIAL CONDITIONS OF CONTRACT (SCC) SUMMARY MATRIX AND SLA 450
SECTION VI-B: DETAILED SPECIAL CONDITIONS OF CONTRACT -- DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION (LOT 2) 461
CLAUSE 1: DEFINITIONS AND INTERPRETATION 461
CLAUSE 2: SCOPE OF CONTRACT 462
CLAUSE 3: SINGLE POINT OF RESPONSIBILITY, CONSORTIUM AND OEM BACK-TO-BACK 463
CLAUSE 4: PROGRAMME GOVERNANCE AND INTERFACE WITH THE LOT 1 PMO 463
CLAUSE 5: REQUIREMENTS BASELINE AND TRACEABILITY 464
CLAUSE 6: CONTRACTOR PERSONNEL 464
CLAUSE 7: SOLUTION STANDARDS AS CONTINUING WARRANTIES 465
CLAUSE 8: SOFTWARE LICENSING, METRICS AND PRICE PROTECTION 466
CLAUSE 9: SAAS SERVICES: SOVEREIGNTY, CONTINUITY AND EXIT 466
CLAUSE 10: INFRASTRUCTURE SUPPLY AND VENDOR-OWNED SIZING 467
CLAUSE 11: OT SYSTEMS, SITE WORKS AND OPERATIONAL SAFETY 467
CLAUSE 12: INTEGRATION RESPONSIBILITIES AND THIRD-PARTY DEPENDENCIES 468
CLAUSE 13: DATA MIGRATION AND QUALITY 468
CLAUSE 14: CUTOVER AND BUSINESS CONTINUITY 468
CLAUSE 15: TESTING AND STAGED ACCEPTANCE 468
CLAUSE 16: PERFORMANCE GUARANTEES 469
CLAUSE 17: CYBERSECURITY AND CRITICAL INFRASTRUCTURE OBLIGATIONS 469
CLAUSE 18: TRAINING, CHANGE MANAGEMENT AND KNOWLEDGE TRANSFER 470
CLAUSE 19: SUPPORT SERVICES AND SERVICE LEVELS 470
CLAUSE 20: LIQUIDATED DAMAGES FOR DELAY 471
CLAUSE 21: PAYMENT, CURRENCY AND PRICE BASIS 471
CLAUSE 22: CHANGE CONTROL AND VARIATIONS 471
CLAUSE 23: INTELLECTUAL PROPERTY 471
CLAUSE 24: INDEMNITIES AND LIMITATION OF LIABILITY 471
CLAUSE 25: DATA PROTECTION, ETHICS AND LOCAL CONTENT 472
CLAUSE 26: TERMINATION, STEP-IN AND EXIT 472
SCHEDULE 1: TESTING (TENDERER TO PROVIDE ALTERNATIVE) 473
1.1 Test Strategy and Governance 473
1.2 Test Stages, Entry/Exit Criteria and Indicative Durations 473
1.3 Defect Management in Testing 474

SCHEDULE 2: DATA MIGRATION (TENDERER TO PROVIDE ALTERNATIVE) 474
2.1 Approach and Phases 474
2.2 Scope of Objects (indicative) 475
2.3 Reconciliation Standards and Tolerances 475
SCHEDULE 3: LICENCE MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE) 475
SCHEDULE 4: PRODUCT ROADMAP AND UPGRADE POLICY (TENDERER TO PROVIDE ALTERNATIVE) 476
SCHEDULE 5: SOFTWARE WARRANTIES (TENDERER TO PROVIDE ALTERNATIVE) 477
SCHEDULE 6: HARDWARE WARRANTIES 477
SCHEDULE 7: RIGHTS TO USE (TENDERER TO PROVIDE ALTERNATIVE) 478
SCHEDULE 8: ACCEPTANCE FRAMEWORK AND TIMELINE (TENDERER TO PROVIDE ALTERNATIVE) 478
8.1A Acceptance Stages and Indicative Timeline (T0 = Effective Date) 479
SCHEDULE 9: QUALITY MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE) 482
SCHEDULE 10: GO-LIVE MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE) 482
10.1 Go-Live Readiness Criteria (per Release/Wave) 482
10.2 Go/No-Go Governance 482
10.3 Cutover Execution 483
10.4 Hypercare 483
SCHEDULE 11: DEFECT LIABILITY AND SUPPORT PERIOD (TENDERER TO PROVIDE ALTERNATIVE) 483
SCHEDULE 12: MILESTONE SIGN-OFF MATRIX (TENDERER TO PROVIDE ALTERNATIVE) 483
SECTION VI-A: SERVICE LEVEL AGREEMENT (SLA) SCHEDULE 484
A. SLA TARGETS AND RESPONSE TIMES 484
B. SYSTEM AVAILABILITY AND UPTIME TARGETS 485
C. PATCH MANAGEMENT AND SECURITY UPDATE TARGETS 485
D. BACKUP, RECOVERY AND BUSINESS CONTINUITY 486
E. REPORTING OBLIGATIONS 486
SECTION VII: CONTRACT FORMS 488
FORM C1: CONTRACT AGREEMENT 488
FORM C2: PERFORMANCE SECURITY (BANK GUARANTEE) 489
FORM C3: PROVISIONAL ACCEPTANCE CERTIFICATE (PAC) 489
FORM C4: FINAL ACCEPTANCE CERTIFICATE (FAC) 490
FORM C5: CHANGE REQUEST AND CHANGE ORDER 490

APPENDIX A — TECHNICAL SPECIFICATIONS/TERMS OF REFERENCE AND PROJECT CHARTER 491
APPENDIX B — BILL OF MATERIALS (BOM) 491
APPENDIX C — APPROVED KEY PERSONNEL 491
APPENDIX D — IMPLEMENTATION PLAN (BASELINE) 492
ANNEXURE A: GLOSSARY OF KEY TERMS 493
ANNEXURE B: KPC PLC ETHICS POLICY SUMMARY 496
ANNEXURE C: CYBERSECURITY REQUIREMENTS FOR IT VENDORS 496
C.1 Information Security Management 496
C.2 Access and Identity Management 496
C.3 Data Security 497
C.4 Vulnerability and Patch Management 497
C.5 Incident Response 497
C.6 Supply Chain Security 497
ANNEXURE D: DATA PROTECTION REQUIREMENTS 497
ANNEXURE E: TENDERER SUBMISSION CHECKLIST 498
ANNEXURE F: CONTACT INFORMATION 499

The document is organised as follows:

- Part 1: Tendering Procedures — Instructions to Tenderers (ITT) and Data Sheet
- Part 2: Tender Forms — Technical Proposal Forms and Financial Proposal Forms
- Part 3: Evaluation Framework — Criteria, Scoring and Methods
- Part 4: General Conditions of Contract for IT Procurement (GCC-IT)
- Part 5: Special Conditions of Contract (SCC) and Service Level Agreement (SLA) Schedule
- Part 6: Contract Forms, Schedules and Annexures
- Annexures: Glossary, Ethics Policy, Cybersecurity Requirements, Data Protection, Tenderer Checklist

PART 1 – TENDERING PROCEDURES

SECTION I: INSTRUCTIONS TO TENDERERS (ITT)

These Instructions govern the preparation, submission, evaluation and award of IT procurement contracts by KPC PLC. Tenderers shall comply fully with these instructions.

A. GENERAL

1. Scope of Tender

1.1 KPC PLC invites tenders for the IT project described in the Data Sheet and Technical Specifications/Terms of Reference. The Tender Reference Number, scope, project type, lot structure (if any) and submission deadline are set out in the Data Sheet.

1.2 IT projects under this STD may be awarded as a single integrated contract (covering hardware, software, licences and services) or as separate lots as specified in the Data Sheet. Where lots are defined, tenderers may bid for one or more lots and evaluation shall be conducted on a lot-by-lot basis.

1.3 KPC PLC may, at its discretion, conduct a Proof of Concept (PoC) or technical demonstration as part of the evaluation process. Where a PoC is required, this shall be specified in the Data Sheet.

2. Definitions

- "AMC" means Annual Maintenance Contract — an agreement for scheduled maintenance, updates and support over a 12-month period;
- "BOM" means Bill of Materials — a detailed list of all hardware, software and licences with quantities and unit prices;
- "Client" means Kenya Pipeline Company PLC (KPC PLC);
- "Cloud Solution" means any IT service delivered over the internet on a subscription or pay-per-use basis, including IaaS, PaaS and SaaS;
- "Custom Development" means software developed specifically for KPC PLC that does not exist as a standard commercial product;
- "Data Sheet" means the document providing tender-specific information supplementing these ITT;
- "Deliverable" means any software, hardware, system, module, report or documentation to be delivered under the Contract;
- "Escrow" means a software source code and documentation deposit with an independent third party for release to KPC PLC upon defined trigger events;
- "GCC-IT" means the General Conditions of Contract for IT Procurement (Section V of this STD);
- "Go-Live" means the date on which the IT system becomes fully operational and accepted by KPC PLC;

- "Licence" means the right granted to KPC PLC to install, use or access software under defined terms;
- "Managed Service" means ongoing IT operational services delivered by the Vendor under a defined SLA;
- "OEM" means Original Equipment Manufacturer — the primary manufacturer of hardware or software;
- "PoC" means Proof of Concept — a demonstration or pilot to validate that a proposed solution meets KPC PLC requirements;
- "SaaS" means Software as a Service — software accessed via the internet on a subscription basis;
- "SLA" means Service Level Agreement — the contractual performance obligations, uptime guarantees and remedies;
- "TCO" means Total Cost of Ownership — the comprehensive financial evaluation of all costs over the system lifecycle;
- "Vendor" means the successful Tenderer awarded the Contract;
- "Warranty" means the period during which the Vendor rectifies defects at no additional cost to KPC PLC;

3. Eligible Tenderers

3.1 This tender is open to IT companies, system integrators, OEM representatives, authorised resellers and managed service providers meeting the eligibility criteria in Section IV, and specifically invited to bid by KPC PLC under a restricted tender process aligned to KPC PLC's internal policies.

3.2 Tenderers may bid as a single firm, a consortium, or a prime contractor with identified subcontractors. The prime contractor shall be fully responsible for all aspects of delivery regardless of subcontracting arrangements.

3.3 A Tenderer shall not be eligible if: debarred by KPC PLC; convicted of corrupt or fraudulent practice; insolvent or under administration; or in material breach of an existing KPC PLC contract.

3.4 OEM Authorisation: Where a Tenderer proposes to supply goods or software of a specific OEM brand, it shall provide a valid OEM Authorisation Letter confirming its status as an authorised reseller or partner for the proposed products. Authorisation shall be current (not expired) at the time of Tender submission.

4. Conflict of Interest

4.1 A Tenderer shall disclose any actual or potential conflict of interest. A conflict includes: involvement in the preparation of Technical Specifications/Terms of Reference for this tender; a financial interest in KPC PLC or its affiliates; or a business arrangement with a KPC PLC employee involved in this procurement.

4.2 A firm that prepared or contributed to the Technical Specifications/Terms of Reference or Project Charter for this procurement shall be disqualified from submitting a tender, unless it can demonstrate that the conflict does not confer an unfair advantage.

5. Corrupt and Fraudulent Practices

5.1 KPC PLC requires the highest standards of ethics from all Tenderers. KPC PLC will reject a Tender and terminate a Contract if corrupt, fraudulent, collusive or coercive practices are discovered. The Ethics Hotline is: report.fraud@kpc.co.ke.

B. PREPARATION OF TENDERS

6. Cost of Tendering

6.1 All costs of preparing and submitting a Tender shall be borne by the Tenderer. KPC PLC is not liable for these costs regardless of the outcome.

7. Language

7.1 All Tenders and related documents shall be in English. Technical data sheets and product documentation from OEMs may be in another language if accompanied by a certified English summary.

8. Documents Comprising the Tender

8.1 A complete Tender submitted through the SAP SRM portal shall comprise:

- Technical Proposal — Forms TP-IT-1 through TP-IT-9 (submitted in the Technical Proposal workspace of the portal)
- **Financial Proposal — Forms FP-IT-1 through FP-IT-2 (submitted in the separate Financial Proposal workspace of the portal — accessible only after Technical Evaluation)**
- Form COI-IT: Conflict of Interest Declaration
- Form BOD-IT: Beneficial Ownership Disclosure
- Form ACD-IT: Anti-Corruption Declaration
- Form DPD-IT: Data Protection and Cybersecurity Compliance Declaration
- Form OEM-IT: OEM Authorisation Letter(s) (where applicable)
- Form CS-IT: Cybersecurity Compliance Statement
- Tender Security (where required by the Data Sheet)
- Any other documents specified in the Data Sheet

9. Lots and Multi-Component Proposals

9.1 Where the Data Sheet specifies that the IT project is divided into lots, Tenderers may bid for one or more lots. Evaluation shall be conducted on a lot-by-lot basis. The Data Sheet specifies whether: (a) a Tenderer may be awarded more than one lot; and (b) whether there is a preference for a single-source award for integration purposes.

9.2 Where the project involves multiple components (hardware, software, services), Tenderers shall price each component separately in the Bill of Materials and Total Cost Schedule but may offer integration discounts for the full project award.

10. Tender Validity and Prices

10.1 Tenders shall remain valid for the period stated in the Data Sheet (minimum 121 days). Prices submitted shall be valid and firm for this period.

10.2 Hardware prices shall be denominated in Kenya Shillings or, where imported equipment is involved, in the currency stated in the Data Sheet. Software licence and SaaS subscription prices may be quoted in USD, EUR, GBP or KES as applicable. The Tenderer shall specify the currency basis and exchange rate assumptions.

10.3 All prices shall be stated inclusive of all applicable taxes, duties, installation, freight, insurance and delivery charges to the KPC PLC site(s) specified.

11. Tender Security

11.1 Where required by the Data Sheet, the Tenderer shall provide a Tender Security valid for 30 days beyond the Tender validity period, in the form of a bank guarantee from a CBK-licensed bank.

12. Clarifications and Pre-Tender Meeting

12.1 Tenderers requiring clarification shall submit written requests through the address provided in the TDS by the clarification deadline stated in the Data Sheet. KPC PLC shall respond to all clarifications in writing via the portal.

12.2 Where a Pre-Tender Meeting or Technical Briefing is scheduled (as stated in the Data Sheet), Tenderers are strongly encouraged to attend. KPC PLC may provide access to the existing IT environment for evaluation purposes, subject to a Non-Disclosure Agreement (NDA).

C. SUBMISSION — DIGITAL-FIRST APPROACH

13. Primary Submission: SAP SRM Portal

13.1 KPC PLC conducts IT procurement through its secure SAP SRM e-procurement portal. The portal is the default submission channel. The portal enforces the tender process rules:

(a) Maintains Technical and Financial Proposals in separate, digitally sealed workspaces — the Financial Proposal workspace is locked until the Technical

Evaluation is formally completed, unless simultaneous opening is permitted and deliberately configured;

(b) Opens all Technical Proposals simultaneously after the submission deadline — no early opening is possible;

(c) Automatically enforces the minimum technical score threshold when configured - Financial Proposals of non-qualifying Tenderers remain sealed;

(d) Provides a structured scoring workflow for the Evaluation Committee with audit trails;

(e) Manages all Tender communications — clarifications, addenda, notifications and award correspondence.

13.2 Tenderers must register on the portal before submission. Registration instructions are at www.kpc.co.ke. Technical difficulties in registration shall be reported to srmsupport@kpc.co.ke at least 5 working days before the submission deadline.

13.3**Uploading Bid Document -** Preferred Submission Method: Tenderers are advised to use the C-Folder for submitting their tenders. This platform is specifically designed to handle bulky technical bid documents of up to100 MB per file.

Exceeding File Size Limit: In the event that the bid response exceeds the 100 MB limit, Tenderers should **Split** their documents into two or more separate files before submission.

14. Physical Submission — Exception Only

14.1 Physical submission is permitted only where explicitly stated in the Data Sheet as a result of exceptional circumstances (such as temporary portal unavailability confirmed by KPC PLC, or for submissions involving classified security documentation). Physical submission is NOT an alternative that Tenderers may elect as a matter of preference.

14.2 Where physical submission applies, the Technical Proposal shall be submitted in a sealed envelope labelled: 'TECHNICAL PROPOSAL — IT TENDER [Reference] — [Tenderer Name] — DO NOT OPEN BEFORE [Date/Time]'. The Financial Proposal shall be in a separately sealed envelope labelled: 'FINANCIAL PROPOSAL — IT TENDER [Reference] — [Tenderer Name] — DO NOT OPEN UNTIL TECHNICAL EVALUATION IS CONCLUDED'. Both envelopes shall be enclosed in an outer sealed envelope addressed to the General Manager- Supply Chain, KPC PLC.

15. Submission Deadline and Late Tenders

15.1 Tenders must be received by the date and time stated in the Data Sheet. The SAP SRM portal automatically rejects late submissions. Physical submissions received after the deadline shall not be opened.

16. Opening of Tenders

16.1 Technical Proposals are opened simultaneously through the SAP SRM portal after the submission deadline and assigned to the Evaluation Committee. Financial Proposals remain

digitally sealed. Where physical opening applies, Technical Proposals may be opened in the presence of Tenderers' representatives who choose to attend.

16.2 Financial Proposals shall be opened only after the Technical Evaluation is complete and minimum threshold qualifying Tenderers have been determined.

D. EVALUATION AND AWARD

17. Evaluation Process Overview

17.1 KPC PLC evaluates IT Tenders in a sequential five-stage process: (1) Preliminary/Administrative Review; (2) Technical Compliance Review; (3) Technical Scoring; (4) Proof of Concept or scripted demonstration (where applicable; for Lot 2, the pass/fail Stage 3B demonstration in Section IV); and (5) Financial/TCO Evaluation. The evaluation shall be conducted by a formally constituted multi-disciplinary Evaluation Committee comprising Supply Chain, IT, Finance and relevant business representatives.

18. Negotiations

18.1 Following evaluation, KPC PLC may conduct negotiations with the recommended Tenderer(s) before award. Negotiations may address: scope refinements; implementation timeline; licence terms; SLA parameters; payment schedule; and TCO optimisation. The fundamental technical requirements and overall project scope shall not be substantially altered through negotiation.

19. Award, Notification and Contract Signing

19.1 KPC PLC shall notify the successful Tenderer in writing that its tender has been accepted. The successful Tenderer shall confirm acceptance in writing within the period stated in the award letter.

19.2 KPC PLC shall simultaneously publish a contract award notice and notify all unsuccessful Tenderers within ten (10) working days of receipt of acceptance by the successful Tenderer. Notification to the unsuccessful tenderers shall be sent via SRM portal.

19.3 Where a Performance Security is required, it shall be provided within 10 working days of tenderer’s confirmation of acceptance.

19.4 KPC PLC reserves the right to award the contract in whole, to award separate lots to different Tenderers, or to reject all Tenders without liability.

E. COMPLAINTS

20. Complaint Mechanism

20.1 A Tenderer who feels aggrieved may submit a written complaint to the General Manager-Supply Chain within five (5) working days of the event. KPC PLC shall acknowledge within five (5) working days and respond substantively within fifteen (15) working days.

SECTION II: TENDER DATA SHEET (TDS)

The Data Sheet provides information specific to each IT procurement. Where there is conflict between the ITT and the Data Sheet, the Data Sheet prevails. KPC PLC staff shall complete this Data Sheet fully before issuing any IT tender.

TDS Reference	Tender-Specific Data
Tender Reference No.	*KPC/PU/OT/134/ICT/NBI/26-27*
Project Title	**Tender For Design, Supply, Implementation, Commissioning, Support and Maintenance Of An Enterprise Digital Solution.**
IT Category	Integrated Project
Project Tier (for evaluation)	Tier 1: Strategic/Mission-Critical
Eligible Tenderers (ITT 3.2)	No Joint Ventures are allowed. A prime contractor may sub-contract other firms to fulfil requirements of this tender. A Lead Firm of a Consortium may team up with other Firms to fulfil requirements of this tender. The Prime Contractor/Lead Firm in a Consortium shall assume end-to-end responsibility for the complete solution, including all proposed software products, licences, infrastructure, interfaces, integrations, custom developments, configurations, migrations, professional services, training, documentation, warranties and support, whether delivered directly or through OEMs, consortium members, subcontractors, affiliates or other third parties. In the event of sub-contracting/Consortium, A detailed teaming agreement with clear responsibilities and dully executed by all parties must be provided The tender is open to both local and foreign firms. The teaming agreement shall explicitly identify the consortium member(s) holding each OEM authorisation and partnership, consistent with the responsibilities assigned to each member. Consortium documentation: every consortium member shall submit a valid tax compliance certificate (or the equivalent for foreign firms), a certificate of incorporation/business registration, and Forms TP-IT-2A, COI-IT, BOD-IT and ACD-IT. Form TP-IT-1B (Consortium Agreement) shall be submitted by the Lead Firm and signed by all members. Subcontractors: tenderers may engage subcontractors of their choice at tender stage. After contract award, the Contractor shall not change or engage new subcontractors without the prior written approval of KPC PLC.
Lot Structure (ITT 9.1)	• **Lot 1 – Provision of Programme Management Services for The Design, Supply, Implementation,**

	Commissioning, Support and Maintenance of an Enterprise Digital Solution • **Lot 2 – Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution.** To preserve the independence of programme governance and ensure effective oversight, **a tenderer shall be permitted to submit Tender for one (1) lot only.** Accordingly: i. A tenderer submitting a bid for **Lot 1** shall not be eligible to submit a bid for **Lot 2**. ii. A tenderer submitting a bid for **Lot 2** shall not be eligible to submit a bid for **Lot 1**. iii. A tenderer shall not participate in more than one submission, whether as a lead respondent, consortium member, subcontractor, affiliate, parent company, subsidiary, or in any other capacity, across both Lots. iv. Where KPC determines that a tenderer has participated in more than one Lot, all affected submissions shall be rejected as non-responsive. v. Each Lot shall be evaluated independently in accordance with the qualification requirements specified in this Tender. vi. A separate tender will be issued to procure an Independent Quality Assurance consultant for the Digital Transformation Project after solutions selection. **The firms who will be awarded LOT 1 and LOT 2 above will not be eligible to participate in the Independent Quality Assurance tender** vii. The one-lot restriction applies to the two Lots of this tender and to the separate Independent Quality Assurance tender. Participation in any other KPC PLC tender does not affect eligibility under this tender.
Additional documents for Technical Submission (ITT 8.1)	All documents indicated as required evidence in the technical evaluation criteria.
Additional documents for Financial Submission (ITT 8.1)	All documents indicated as required evidence in the financial evaluation criteria.
Proof of Concept / Scripted Demonstration (ITT 17.1)	Lot 1: not applicable. Lot 2: required
Minimum Technical Score (ITT 17.1)	i. Tenderers may be disqualified at any stage of evaluation for any non-conformity to mandatory, technical and functional requirements. ii. Lot 1: a minimum technical score of 75% is required for financial evaluation.

	iii. Lot 2: a minimum technical score of 75% is required at Stage 3A to proceed to stage 3B, and a pass in every Stage 3B demonstration script is required to progress to financial evaluation.
Technical: Financial Weighting (ITT 17.1)	i. Lot 1: Technical 80%: Financial 20%. ii. Lot 2: Technical 80%: Financial 20%. iii. The Tenderer achieving the highest Final Combined Evaluation Score shall be ranked first and may be considered for award.
TCO Evaluation Period (ITT 17.1)	6 years
Submission Method (ITT 13.1)	Completed tenders must be submitted electronically in PDF format and uploaded on the Supplier Relationship Management (SRM) Collaboration Folder, Using the link https://e-procurement.kpc.co.ke/irj/portal. **Instructions to Tenderers: Caution on Uploading Bid Documents** **a)** Preferred Submission Method: Tenderers **MUST** use the **C-Folder to submit their technical bids**. This platform is specifically designed to handle bulky Technical bid documents. **b)** The Financial bids **MUST** be submitted through the Note and Attachments tab. Files exceeding 100MBS Size Limit should be **Split** into smaller files not exceeding 100MBS each. This ensures the integrity of the tendering process and accurate evaluation of all necessary information. Manuals to guide on the bidding process are accessible via the KPC website www.kpc.co.ke under Tenders
Tender Submission Deadline (ITT 15.1)	**30th November 2026 at 10:00 AM EAT**
Clarification Deadline (ITT 12.1)	All requests for clarification shall be received by KPC PLC not later than five (5) days before the tender submission deadline. Where the submission deadline is extended, the clarification deadline shall be computed from the new submission deadline.
Site Visit / Lab Access	Optional for all sites listed below. Visits shall commence at 10:00 hrs EAT, except PS09 Embakasi JKIA Depot, which shall be visited after PS10 on the same day at 14:00 hrs.

	<table><tr><th>No.</th><th>STATION</th><th>DATE</th></tr><tr><td>1.</td><td>PS10 & PS09</td><td>20. 11.2026</td></tr><tr><td>2.</td><td>PS25</td><td>23. 11.2026</td></tr><tr><td>3.</td><td>PS27</td><td>24.11.2026</td></tr><tr><td>4.</td><td>Ps28</td><td>24.11.2026</td></tr></table> All participants shall carry valid identification (national ID or passport) and wear appropriate PPE: cotton overalls or dust coats, leather safety boots and hard hat. Cameras shall not be allowed within KPC terminals. Site visits are held once only; no repeat or additional visits shall be arranged. Detailed site information not obtainable at the site visit shall be provided during blueprinting.
Tender Validity (ITT 10.1)	121 calendar days from the tender submission deadline
Tender Security (ITT 11.1)	**Required: USD 50,000 —** Bank Guarantee from a bank licensed by the Central Bank of Kenya (CBK), in the format of the Tender Security Form, valid for 151 days from the date of tender opening. • A tender security issued by a CBK-licensed bank against a counter-guarantee from a foreign bank is acceptable, provided that the guarantee submitted to KPC PLC is issued by the Kenyan bank in its own name and constitutes an irrevocable, unconditional and payable-on-first-demand obligation of that bank. KPC PLC's right of recourse shall be solely against the issuing Kenyan bank, and payment shall not be subject to the performance or reimbursement obligations of the foreign counter-guaranteeing bank. The same rule applies to the Performance Security. • Tenderers must submit a scanned copy of the tender security with their bid. • The original tender security must be dropped in the tender box on the ground floor, Kenpipe Plaza, Sekondi Road off Nanyuki Road, Industrial Area, Nairobi **on or before date and time of tender opening 10:00 am 30th November 2026** . • Tenderers are advised to note any change in the tender opening date and extend the security accordingly.
Currency of Tender — Hardware (ITT 10.2)	USD The currency that shall be used for Tender evaluation and comparison purposes to convert at the selling exchange rate all Tender prices expressed in various currencies into a single currency is USD

	The source of exchange rate shall be: The Central Bank of Kenya (Mean Rate) The date for the exchange rate shall be the date of tender opening.
Currency of Tender — Software/SaaS (ITT 10.2)	USD The currency that shall be used for Tender evaluation and comparison purposes to convert at the selling exchange rate all Tender prices expressed in various currencies into a single currency is USD The source of exchange rate shall be: The Central Bank of Kenya (Mean Rate) The date for the exchange rate shall be: the date of tender opening.
Delivery Location(s)	KPC Head Office, Nairobi and other stations provided in the Terms of Reference.
Implementation Timeline	Implementation period of at most eighteen (18) months, measured from the date of project kick-off (as agreed by both parties at contracting) to Go-Live. The Go-Live declaration triggers the Warranty and Hypercare periods.
Warranty Period	i. Minimum three (3) years warranty for all equipment (hardware) supplied, including on-site support at the terminals for three (3) years. Stocking of spares shall be specified in the SLA. **ii.** Warranty period for software shall be equivalent to the subscription duration.
Support Contract Duration	Hardware support: three (3) years. Consulting/application support for configurations: two (2) years. OEM software maintenance support: three (3) years for subscription, cloud and perpetual licences. Renewable at KPC PLC's option.
Licence Terms	The contract term for subscription licences and services shall be three (3) years, renewable once at the same cost. Unit prices for subscriptions, support and renewals shall be fixed for six (6) years (two three-year terms) from first Production Go-Live. Any growth in quantities shall be charged at the fixed unit prices. Tenderers shall state their pricing assumptions.
SLA Response Times	Refer to the SLA Schedule (Section VI-A) of the Tender Document.
Performance Security (ITT 19.3)	Required: 10% of Contract Price — Bank Guarantee from a CBK-licensed bank, valid up to ninety (90) days after issue of the Final Acceptance Certificate.

SECTION II-A: TERMS OF REFERENCE

1.0 Introduction of KPC

Kenya Pipeline Company PLC (KPC PLC) is a publicly listed company incorporated in the Republic of Kenya and operating within the midstream segment of the oil and gas value chain. Since commencing commercial operations in 1978, the Company has played a strategic role in the transportation, storage, and management of petroleum products across Kenya and the wider East and Central African region.

KPC operates under the regulatory oversight of various national institutions including the Energy and Petroleum Regulatory Authority (EPRA), the Capital Markets Authority (CMA) and other applicable government and regulatory agencies.

The Company is the primary transporter of refined petroleum products in Kenya and operates an extensive pipeline network, pumping stations, terminals, aviation fuel facilities, and storage depots strategically located across the country.

KPC manages a national pipeline network of approximately 1,342 kilometres with a storage capacity exceeding 1.14 million cubic metres. The pipeline network facilitates transportation of refined petroleum products from the coastal region to Nairobi and onward to western Kenya and regional markets including Uganda, Rwanda, Burundi, South Sudan, eastern Democratic Republic of Congo, and northern Tanzania.

The Company also operates an aviation fuel infrastructure supporting major airports including Jomo Kenyatta International Airport (JKIA) and Moi International Airport (MIA).

As a strategic national infrastructure entity, KPC plays a critical role in national energy security, regional trade facilitation, petroleum supply stability, and economic development.

1.0.1 Core Business Functions

KPC executes its mandate through integrated operational, commercial, technical, and corporate functions that collectively support the efficient transportation, storage, management, and distribution of petroleum products.

Core operational functions include:
i. Pipeline transportation and product movement management;
ii. Depot and terminal operations management;
iii. Petroleum storage and inventory management;
iv. Aviation fuel operations;
v. Scheduling and nomination management;
vi. Product quality assurance and laboratory management;
vii. Engineering, maintenance, and asset integrity management;
viii. Custody transfer and metering operations;
ix. Operational monitoring and control through SCADA and automation systems;
x. Commercial operations including billing, invoicing, and customer account management; and
xi. Regional petroleum logistics coordination.

Supporting corporate functions include:
i. Financial management and treasury operations;

ii. Procurement and supply chain management;
iii. Human resource and payroll management;
iv. Legal, compliance, and risk management;
v. Enterprise ICT and cybersecurity management;
vi. Project management and infrastructure development;
vii. Governance and performance management; and
viii. Environmental, health, safety, and sustainability management.

These functions operate within a highly regulated and operationally sensitive environment requiring high levels of reliability, integration, operational visibility, cybersecurity, and business continuity.

1.0.2 Business Model

KPC operates a complex midstream petroleum logistics and storage business model supporting both domestic and regional markets.

Key operational characteristics include:
i. Operation of custom bonded warehouses and regulated petroleum storage facilities;
ii. Management of commingled petroleum products and interface handling within multiproduct pipeline systems;
iii. Oil banking operations (exchanges, in-tank trading, collateral financing, global book inventory/fungible products, physical inventory, multilevel approvals, line-fill, product categories and tax categories) and strategic petroleum stock management;
iv. Multiproduct pipeline transportation, scheduling, and terminal operations;
v. Batch-based product quality inspection and certification processes;
vi. Gain and loss management across transportation and storage operations;
vii. Real-time integration with regulatory and revenue collection systems including KRA platforms; and
viii. Support for regional petroleum distribution to multiple destinations across East and Central Africa.

1.0.3 Organizational Structure and Business Units

KPC operates through interdependent operational and support functions that collectively deliver the Company’s mandate.

The Operations and Pipeline Management function oversees pipeline transportation, depot operations, product movement management, scheduling, and operational control systems including SCADA and automation environments.

The Engineering and Projects function is responsible for infrastructure development, maintenance engineering, asset lifecycle management, integrity management, and execution of strategic capital projects.

The Commercial and Marketing function manages customer engagement, tariff administration, billing, contractual management, and regional commercial relationships.

The Finance function manages accounting, treasury operations, budgeting, financial reporting, taxation, and financial governance.

The Supply Chain Management function oversees procurement, inventory management, warehousing, supplier management, and contract execution.

The Information and Communication Technology function supports enterprise systems, infrastructure, cybersecurity, operational technology integration, enterprise architecture, and digital transformation initiatives.

The Legal, Compliance, and Risk function oversees governance, legal advisory services, regulatory compliance, enterprise risk management, and corporate governance.

The Human Resources and Administration function supports workforce management, payroll, talent development, administration, and organizational performance management.

1.0.4 Geographical Coverage

KPC operates an extensive infrastructure network supporting both national and regional petroleum distribution operations.

Within Kenya, operations span strategic locations including Mombasa, Nairobi, Nakuru, Eldoret, Kisumu, and aviation fuel facilities at major airports.

The Company also supports regional petroleum supply and logistics operations serving neighboring countries within the East and Central African region.

Through integration of pipeline, road, rail, and lake transport systems, KPC serves as a critical logistics enabler within the Northern Corridor regional trade network.

1.0.5 Workforce

KPC employs a multidisciplinary workforce supporting operational, technical, commercial, and corporate functions across the organization.

The workforce comprises professionals in engineering, operations, information and communication technology, finance, supply chain management, commercial operations, legal and compliance, customer service, and field operations.

Technical personnel include pipeline, instrumentation, mechanical, electrical, automation, and ICT specialists responsible for the operation, maintenance, monitoring, and modernization of pipeline and terminal infrastructure.

The Company workforce is distributed across the head office, depots, pumping stations, aviation fuel facilities, regional offices, and operational sites across the country.

The approximate workforce size and user population applicable to this project shall be provided in the detailed requirements and sizing sections of this Tender.

1.0.6 Key Stakeholders

KPC operates within a broad stakeholder ecosystem reflecting its strategic role within the national and regional energy sector.

Below is a list of key stakeholders

Stakeholder	Stakeholder Requirements / Modules
Government ministries	Government reporting and stakeholder communications.
Regulatory Institution – CMA	Regulatory compliance, reporting and disclosures.
Regulatory Institution – EPRA	Regulatory compliance, licensing and reporting.
Regulatory Institution – NEMA	Environmental compliance and ESIA management.
Tax Authorities (KRA, URA, RRA)	Tax management and statutory reporting.
Energy and petroleum sector regulators;	Regulatory reporting, licensing and compliance.
Oil Marketing Companies (OMCs);	OMC Portal
Regional petroleum distribution partners;	Petroleum logistics and information exchange.
Financial Institutions and development partners;	Bank interfaces and financial transactions.
Customers and logistics stakeholders;	CRM and customer service management.
Internal management and employees;	Employee, workflow and management services
Shareholders and investors;	Investor relations and shareholder communications.
Technology and infrastructure partners;	Integration, technical support and service management.
National security, regulatory, and critical infrastructure institutions.	Secure information exchange and compliance

1.0.7 Current Systems and Enterprise Technology Landscape

KPC currently operates a diverse and evolving enterprise and operational technology environment comprising business systems, operational systems, integration platforms, infrastructure platforms, and supporting technologies that collectively support its operations.

The current environment has evolved over time through multiple implementation phases, integrations, and custom developments, resulting in varying levels of maturity, integration, automation, scalability, operational efficiency, and maintainability.

The technology landscape includes enterprise resource planning systems, operational technology systems, integration platforms, analytics environments, infrastructure platforms, cybersecurity solutions, and various business support applications supporting both corporate and operational functions.

1.0.8 Enterprise Systems Landscape

The Company's core enterprise systems are primarily based on enterprise ERP technologies supporting finance, procurement, supply chain management, maintenance, human resource management, analytics, and operational support functions.

The current enterprise environment includes ERP platforms, procurement systems, contract lifecycle management systems, reporting platforms, document and records management systems, integration platforms, and various supporting business applications.

The environment contains significant levels of customization, integrations, workflows, reports, extensions, and operational enhancements developed over time to support KPC-specific business processes and operational requirements.

Current enterprise systems landscape:

System / Module	Description	Key Dependencies / Customisations
SAP IS-Oil & Gas (OIL), Quantityware,	Industry solution supporting bulk scheduling, silo management, nominations and ticketing, transport and distribution, shipment planning, truck and drivers master data, and terminal distribution processes, including quantity and Quantityware Conversion (QCI), trading and scheduling (TSW), and hydrocarbon product management (HPM) functionality, TD for shipments management and online portal for order entry and reporting.	Extensive enhancements including custom BAPIs, user exits, and operational integrations across IS-Oil, Quantityware, and TSW/HPM components
Custom Trucks Queue Management System (QMS) with Displays	Trucks Queue Management System	Truck Availability, Security Checks , Safety Inspections, and Order Queueing with displays and mobile phones interfaces.
SAP FI / CO and Funds Management	Financial accounting, controlling, budgeting, and treasury processes	Custom financial reports, localization enhancements, and reconciliation processes
SAP MM, MM-OPS and SRM	Procurement, inventory management, and warehouse operations	Custom stock reconciliation and wet-stock management processes
SAP Sales Distribution (SD)	Sales, billing, pricing, and commercial operations	Custom pricing procedures and operational integrations
SAP PM and SAP PS	Enterprise asset and maintenance management and Project Management	Integration with operational monitoring and SCADA environments
SAP QM	Product quality management and laboratory processes	Integration with laboratory and testing systems

System / Module	Description	Key Dependencies / Customisations
HR / Payroll/ ESS/ MSS	Human resource and payroll management, including Employee Self-Service (ESS) and Manager Self-Service (MSS) portals for leave, time, and personnel data management	Local payroll and statutory compliance customizations, and custom ESS/MSS workflow configurations
Power BI	Enterprise reporting and presentation platform	Custom analytics models, dashboards, and reporting structures
SAP GRC	Governance, risk, and compliance management, including access control, risk management, and audit management	Custom segregation-of-duties (SoD) rules and access control workflows integrated with core SAP modules
SAP PO	Process Orchestration middleware for integration between SAP and non-SAP systems	Custom interfaces and integration scenarios connecting SAP with third-party and legacy systems
SAP HCM, Payroll	Core HR master data, organizational management, and payroll processing	Custom payroll schemas and country-specific statutory reporting configurations
SAP Solution Manager	Centralized platform for system monitoring, Systems Change Request Management, application lifecycle management, and technical landscape administration	Custom monitoring configurations and integration with operational support processes
SAP Fiori	Role-based user interface layer providing responsive, simplified access to SAP transactions and workflows	Custom Fiori app configurations and launchpad integrations tailored to business roles
List of Custom Applications within SAP and Other Environments	Safety Observation and Corrective Action E-Recruitment Industrial Attachment Management Visitor Management System Flight Request Management Task Assignment and Monitoring Incidents Management Security Seals Management Medical and Clinic Management Risk Management Insurance Claims Management Loan Application Boardroom Managements Fleet Management FOC Onboarding Claims Requests Payment Requests ICT Equipment Request Application Capacity Planning	Bespoke, non-standard applications developed in-house and integrated with the core SAP landscape (primarily via SAP PO and Fiori) to support business-specific processes not covered by standard SAP functionality. Customisations include tailored workflows, approval hierarchies, notifications, and role-based access controls, with data integrations to relevant SAP modules (e.g., HCM, GRC, PM/PS) and other enterprise systems as required by each application.
SAP Technical	SAP BASIS	Underlying technical layer supporting system administration, performance monitoring, security, and transport management across all SAP modules; customised system landscape and interface configurations.

System / Module	Description	Key Dependencies / Customisations
OT Systems	i. SCADA, ii. Fuelfacs, iii. Integrated Security System for Clock-in/out and CCTV iv. Tank Guaging System v. GIS vi. Leak Detection System (LDS)	Operational technology systems interfaced with SAP for asset and maintenance data; custom interfaces for real-time data exchange between OT and SAP environments.

1.0.9 Operational Technology (OT) Landscape

KPC operates specialized operational technology platforms and industrial systems supporting pipeline transportation, terminal operations, inventory management, automation, monitoring, and operational control.

The OT environment includes SCADA systems, automation systems, telemetry systems, tank gauging systems, custody transfer systems, metering systems, scheduling systems, pipeline optimization systems, and other industrial control technologies supporting real-time operational management.

Operational systems are tightly integrated with enterprise systems to support stock accounting, scheduling, maintenance management, operational visibility, reconciliation, billing, and regulatory reporting.

The operational environment also supports integration with laboratory systems, weighbridge systems, fleet management systems, banking systems, and government regulatory platforms.

1.0.10 Integration Landscape

KPC currently operates a hybrid integration environment supporting integration between enterprise systems, operational technology platforms, external stakeholders, banking systems, regulatory systems, and third-party platforms.

The current environment supports API-based, file-based, event-driven, and message-based integration models enabling data exchange across business and operational functions.

Integration landscape:

System	Vendor/Version	Datasets	Notes/Protocols
SCADA / Historian	Aveva/Schneider Electric	Nominations, Metered Quantities, Equipment status (Maintenance) , SCADA Historian data	OPC DA for real-time data; ODBC/SQL for historian/database access.
Automatic Tank Gauging (ATG)	Rosemount / Emerson	Tank Inventory Data	ODBC connection to SQL Database

System	Vendor/Version	Datasets	Notes/Protocols
TAS - FuelFACS/Honeywell	Guidant	Loading orders; master data; transaction status; density; loading results	ODBC/SQL, file interfaces including SFTP/Robocopy
GIS		Depot/station locations; tanks; pipelines; routes; infrastructure/assets; geospatial coordinates	REST/API, OGC services, database connection or file exchange
Preset / Batch Loading Controller	Smith Meter AccuLoad	Order data, metered quantities, density & temperature	SMIP / Smith Meter protocol and/or Modbus TCP
Automatic Number Plate Recognition (ANPR)		Vehicle Number plates, Timestamps (entry&exit)	REST API
Biometric / Access Control System		Staff identification; access events; clock-in/out; driver access events; authentication results	API / database / file interface
TeamMate+/ Arbutus		Audit transactions; operational/financial data;	ODBC/database connections, adapters, scripts, file imports
KRA iCMS		Loading booking data; loaded quantities; gate-pass information; customs/transaction information	SOAP/XML web service (iCMSService), with Action identifying the transaction and RequestMsg carrying the XML business payload in CDATA.
KRA TIMS		Invoice information; tax invoice data; fiscalization/transaction information	RESTful web service using HTTP POST, transmitting invoice data in JSON format.
KRA iTAX		Withholding tax/VAT, Payment Registration Number	File download
Banks		Payment transactions; account statements; MT940/MT942; payment confirmations; reconciliation data	SFTP/file exchange, API, IDOC
Hydrant Management Systems		Hydrant loading orders; loading authorization; metered quantities; transaction status	ODBC/database
Security Information and Event Management (SIEM)	Fortinet	Security events; authentication events; application logs; API logs; audit trails; network events; integration and middleware events; security alerts and incidents	Syslog; REST API; SIEM connectors; agent-based or agentless log forwarding; event streaming

System	Vendor/Version	Datasets	Notes/Protocols
Identity and Access Management (IAM)	One Identity	User identities; employee accounts; roles; permissions; access rights; authentication events; provisioning and deprovisioning data	LDAP/Active Directory; SAML; OAuth 2.0; OpenID Connect; REST API; SCIM

The current integration environment relies on enterprise middleware and integration technologies to facilitate interoperability between enterprise systems, operational systems, external stakeholders, and third-party platforms.

1.0.11 Data, Reporting, and Analytics

Data and reporting capabilities are currently distributed across multiple enterprise and operational systems with varying levels of consolidation, standardization, governance, and automation.

The current environment includes operational reporting, financial reporting, management dashboards, regulatory reporting, and analytics capabilities. However, enterprise-wide data consolidation, advanced predictive analytics, real-time operational intelligence, and centralized reporting capabilities remain limited.

Data is currently distributed across multiple operational and enterprise systems, resulting in reporting inconsistencies, data duplication, limited visibility, and challenges in achieving a unified enterprise-wide view of operations and performance.

The current environment also presents challenges relating to:
i. Data quality and consistency across systems;
ii. Limited real-time analytics and operational visibility;
iii. Fragmented reporting platforms and dashboards;
iv. Limited predictive and prescriptive analytics capabilities;
v. Manual data consolidation and reconciliation processes;
vi. Limited enterprise data governance and master data management capabilities; and
vii. Limited AI/ML-enabled operational and business intelligence capabilities.

The transformation initiative seeks to establish an integrated enterprise data platform supporting centralized reporting, enterprise analytics, AI/ML capabilities, operational intelligence, executive dashboards, predictive analytics, and data-driven decision-making across the organization.

1.0.12 Customization Landscape

The current enterprise systems environment contains substantial levels of customization, extensions, integrations, workflows, reports, and enhancements developed over time to support KPC-specific operational, commercial, regulatory, and reporting requirements.

These custom developments support industry-specific operational processes, localization requirements, workflow automation, regulatory reporting, integration requirements, and operational decision-making processes.

Customization landscape:

Customisation Type	Approximate Volume	Current Business Justification
Custom Data Structures and Extensions	~85	Industry-specific operational extensions
User Exits, BADIs, and Enhancements	~120	Functional gaps, localization, and operational requirements
Custom Programs, Reports, and Forms	~200+	Operational reporting and regulatory reporting
Workflow Configurations	~18	Approval and operational workflow processes
Integration Interfaces and Flows	~45	Enterprise and operational integrations
Custom Pricing and Billing Logic	~15	Commercial and regulatory pricing requirements
Analytics Models and Reporting Structures	~60	KPI reporting and operational analytics

The proposed transformation initiative is expected to rationalize and optimize the current customization landscape by adopting standardized, configurable, scalable, and maintainable enterprise capabilities while minimizing unnecessary custom developments wherever feasible.

1.0.13 Infrastructure Landscape

KPC's ICT infrastructure is predominantly hosted within on-premise data centre environments comprising enterprise compute, storage, network, virtualization, security, backup, and disaster recovery platforms.

The infrastructure environment consists of a combination of legacy and modern technologies supporting enterprise applications, operational systems, databases, integration platforms, analytics environments, and cybersecurity services.

Cloud adoption within the current environment remains limited and primarily focused on selected collaboration, analytics, and external-facing services.

The current infrastructure environment presents opportunities for modernization, scalability improvement, resilience enhancement, operational optimization, and improved cybersecurity capabilities.

The environment also presents increasing requirements relating to:
i. High availability and operational resilience;
ii. Disaster recovery and business continuity;

iii. Enterprise cybersecurity and Zero Trust security architecture;
iv. Secure IT and OT convergence;
v. Centralized monitoring and observability;
vi. Immutable backup and recovery capabilities;
vii. Infrastructure scalability and performance optimization; and
viii. Compliance with data protection, cybersecurity, and critical infrastructure regulations.

1.0.14 Current Challenges

The current enterprise and operational systems landscape present several operational, technical, integration, and strategic challenges.

These challenges include:
i. Fragmented systems and limited end-to-end integration across business and operational functions;
ii. Significant dependence on manual or semi-automated business processes;
iii. Limited real-time operational visibility and enterprise-wide analytics capabilities;
iv. Data silos and inconsistent reporting structures across systems;
v. High maintenance and operational support complexity arising from legacy platforms and extensive customizations;
vi. Limited scalability and flexibility to support future business growth and digital innovation;
vii. Increasing cybersecurity, compliance, and operational resilience requirements;
viii. Limited predictive analytics and intelligent operational optimization capabilities;
ix. Limited enterprise-wide observability and monitoring capabilities; and
x. Challenges in achieving a unified enterprise-wide view of operations, performance, and decision support.

2.0 Digital Transformation Project

In response to the current operational, technological, regulatory, and business challenges, KPC is undertaking a comprehensive enterprise digital transformation programme aimed at modernizing its enterprise architecture, operational technology environment, business processes, analytics capabilities, and cybersecurity posture.

The transformation initiative seeks to establish a secure, scalable, integrated, and future-ready enterprise technology environment capable of supporting operational excellence, business growth, resilience, compliance, sustainability, and digital innovation.

The broad objective of this project is to:

i. Replace fragmented and legacy systems with an integrated enterprise platform.
ii. Enable seamless integration between enterprise systems and operational technology environments.
iii. Improve operational efficiency and achieve 1.5% increase in throughput.
iv. Enhance real-time operational visibility, analytics, and decision support capabilities.
v. Strengthen cybersecurity, governance, and regulatory compliance capabilities;
vi. Support predictive analytics, AI/ML-enabled optimization, intelligent automation, and operational intelligence capabilities;

vii. Improve user experience and enterprise collaboration;
viii. Support business continuity, resilience, and disaster recovery objectives;
ix. Support digital twin, pipeline optimization, predictive maintenance, and intelligent scheduling capabilities.
x. Establish a scalable technology foundation aligned to KPC's long-term strategic objectives.

2.0.1 Project Overview

Kenya Pipeline Company PLC (KPC) is undertaking an Enterprise Digital Transformation Programme to modernize its business processes, operational systems, digital capabilities and ICT infrastructure through the implementation of integrated digital platforms that support operational excellence, regulatory compliance, cybersecurity and data sovereignty. The Programme comprises two (2) independent Lots, namely:

a. **LOT 1 – Provision of Programme Management Services for The Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution.**

b. **LOT 2 – Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution.**

The Enterprise Digital Transformation Programme comprises multiple interdependent systems, including enterprise business applications, Mid-Stream Oil Operations Systems (MSOOS), ICT infrastructure modernization, enterprise integration services, enterprise data and analytics platforms, cybersecurity capabilities, data migration, organizational change management, training, testing, deployment, post-implementation support and other associated professional services.
Given the strategic importance, complexity, scale and multi-vendor nature of the Programme, KPC intends to appoint an independent Programme Management Office (PMO) to provide programme governance, programme management, project controls, quality assurance, contract administration support, implementation oversight, risk management, benefits realization monitoring and advisory services throughout the Programme lifecycle.

2.0.2 Roles and Responsibilities

2.0.2.1 *General Governance*

KPC intends to appoint an independent Programme Management Office (PMO) to provide programme governance, programme management, project controls, quality assurance, contract administration support, implementation oversight, risk management, benefits realization monitoring and advisory services throughout the Programme lifecycle.
The PMO shall serve as KPC's independent Programme Management Office and assurance partner throughout the Enterprise Digital Transformation Programme.
The PMO shall provide programme governance, project controls, coordination, quality assurance, contract administration support, programme reporting and advisory services while KPC retains overall ownership, accountability and decision-making authority for the Programme.
The PMO shall not undertake implementation activities that form part of the Enterprise Digital Transformation Solution Contractor's obligations.
The contractor for the Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution shall remain solely responsible for solution design, software implementation, systems integration, infrastructure deployment, testing, data migration, training, deployment, warranty and post-implementation support.
An independent quality assurance consultant shall be onboarded at a later stage.

2.0.2.2 *Responsibilities of the PMO*

The PMO shall perform, at a minimum, the responsibilities shown below.

No.	Service Area	Responsibilities
1	Programme Governance	Establish, administer and continuously improve the Programme Governance Framework.
2	Programme Planning	Develop, maintain and monitor the Integrated Master Programme Plan and implementation baselines.
3	Programme Coordination	Coordinate implementation activities across all programme workstreams, contractors and stakeholders.
4	Programme Controls	Monitor programme scope, schedule, budget, quality, resources and benefits realization.
5	Risk, Issue and Change Management	Maintain programme RAID Registers, Decision Registers and Change Registers and coordinate mitigation activities.
6	Contract Administration Support	Monitor implementation contractor compliance with contractual obligations, milestones, deliverables and Service Levels and provide recommendations to KPC.
7	Quality Assurance	Conduct independent reviews of deliverables, solution designs, implementation activities, testing outcomes and programme documentation.
8	Architecture Assurance	Coordinate technical reviews to ensure compliance with approved enterprise architecture, standards and design principles.
9	Business Readiness	Monitor organizational readiness, stakeholder engagement, communications, training and user adoption.
10	Data Migration Assurance	Review migration strategy, migration execution, reconciliation and cutover readiness.
11	Testing Assurance	Monitor governance of System Integration Testing, User Acceptance Testing, Performance Testing and Operational Readiness Testing.
12	Go-Live Assurance	Conduct deployment readiness assessments and monitor stabilization activities.
13	Benefits Realization	Monitor realization of approved programme benefits and strategic objectives.
14	Executive Reporting	Prepare dashboards, reports, decision papers and presentations for Programme Governance Bodies.
15	Milestone Verification	Verify completion of implementation milestones and recommend certification of milestone achievement prior to payment approval.

2.0.2.3 *Responsibilities of Kenya Pipeline Company PLC*

KPC shall be responsible for the following.

1. Provide executive sponsorship and strategic direction for the Programme.
2. Establish and maintain the Programme Governance Structure.
3. Appoint Programme Sponsors, Business Owners, Project Managers and Subject Matter Experts.
4. Review and approve programme deliverables, stage gates and governance decisions.
5. Provide timely access to business users, information, systems, facilities and documentation.
6. Facilitate stakeholder participation during requirements gathering, design reviews, testing, build, training and change management activities.
7. Review submitted deliverables and provide comments within the agreed review periods.
8. Manage internal communications, policy decisions and organizational approvals.
9. Administer contracts and certify payments in accordance with the Conditions of Contract.
10. Approve implementation milestones and final acceptance of contractual deliverables.

2.0.2.4 *Responsibilities of the Enterprise Digital Transformation Solution Contractor*

The Enterprise Digital Transformation Solution Contractor shall be responsible for, but not limited to, the following.

1. Solution design and enterprise architecture.
2. Business process analysis and solution configuration.
3. Supply, installation and commissioning of software and ICT infrastructure.
4. Systems integration and interface development.
5. Data migration and reconciliation.
6. Development and execution of testing activities.
7. Training and organizational change management.
8. Cutover planning and production deployment.
9. Hypercare and warranty support.
10. Operational handover and post-implementation support.
11. Delivery of all contractual deliverables in accordance with the approved implementation plan.
12. Compliance with all contractual milestones, Service Levels, Technical Specifications/Terms of Reference and quality requirements.

The Contractor shall cooperate fully with the PMO and provide unrestricted access to implementation schedules, project documentation, reports, risks, issues, testing results, programme metrics and other information necessary to support effective programme governance and independent assurance.

2.0.2.5 *End-to-End Solution Responsibility*

The Lead Contractor/firm shall assume end-to-end responsibility for the successful delivery and operation of the complete Enterprise Digital Transformation Solution.

The Lead Contractor/firm shall remain fully accountable for all proposed products, software, licences, subscriptions, infrastructure, interfaces, integrations, custom developments, configurations, data migration activities, professional services, deliverables and dependencies, irrespective of whether these are provided directly by the Contractor or through OEMs, consortium members, subcontractors, affiliates or other third parties.

All components necessary to achieve a complete, integrated and operational Solution shall be deemed included within the Contractor's scope, whether or not each individual component is expressly identified in the technical requirements or Bill of Materials.

2.0.2.6 *Collaboration Requirements*

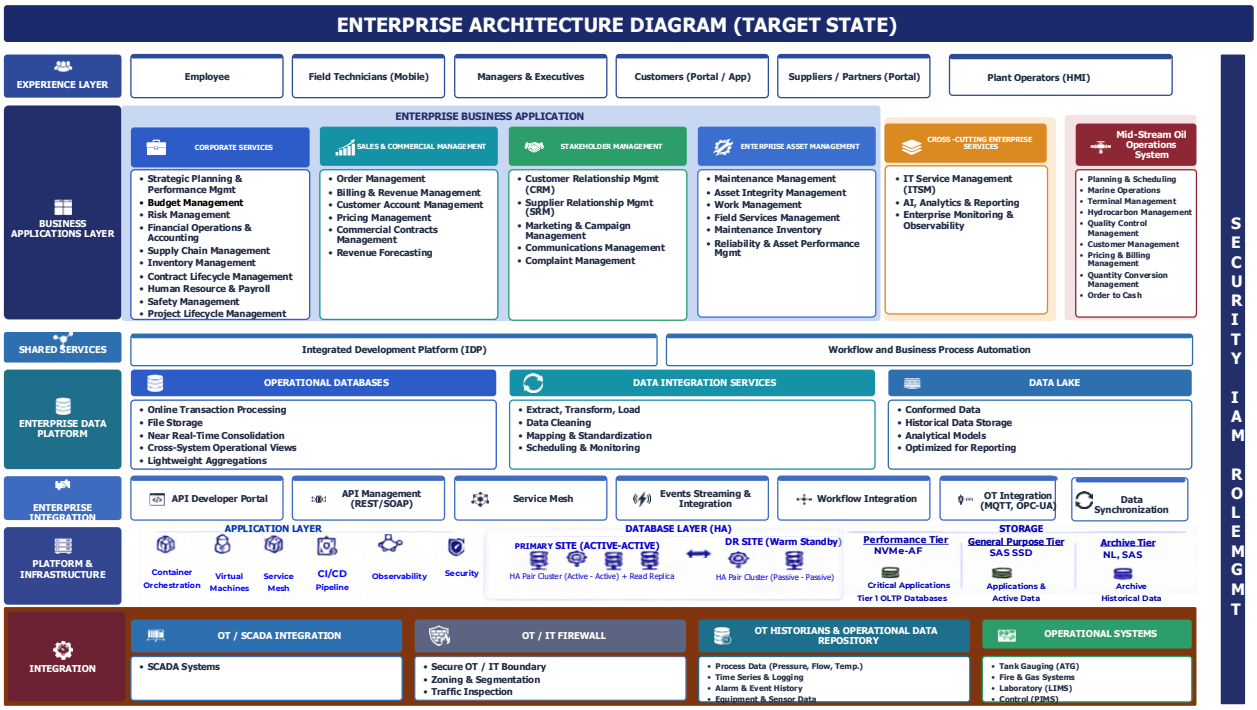
The PMO shall work collaboratively with the following stakeholders throughout the Programme.

No.	Stakeholder
1	KPC Board and Executive Management
2	Programme Steering Committee
3	Programme Management Committee
4	Business Process Owners
5	ICT Department
6	Enterprise Digital Transformation Solution Contractor(s)
7	Original Equipment Manufacturers (OEMs)
8	Infrastructure and Technology Vendors
9	External Consultants
10	Internal and External Auditors
11	Regulatory Authorities, where applicable

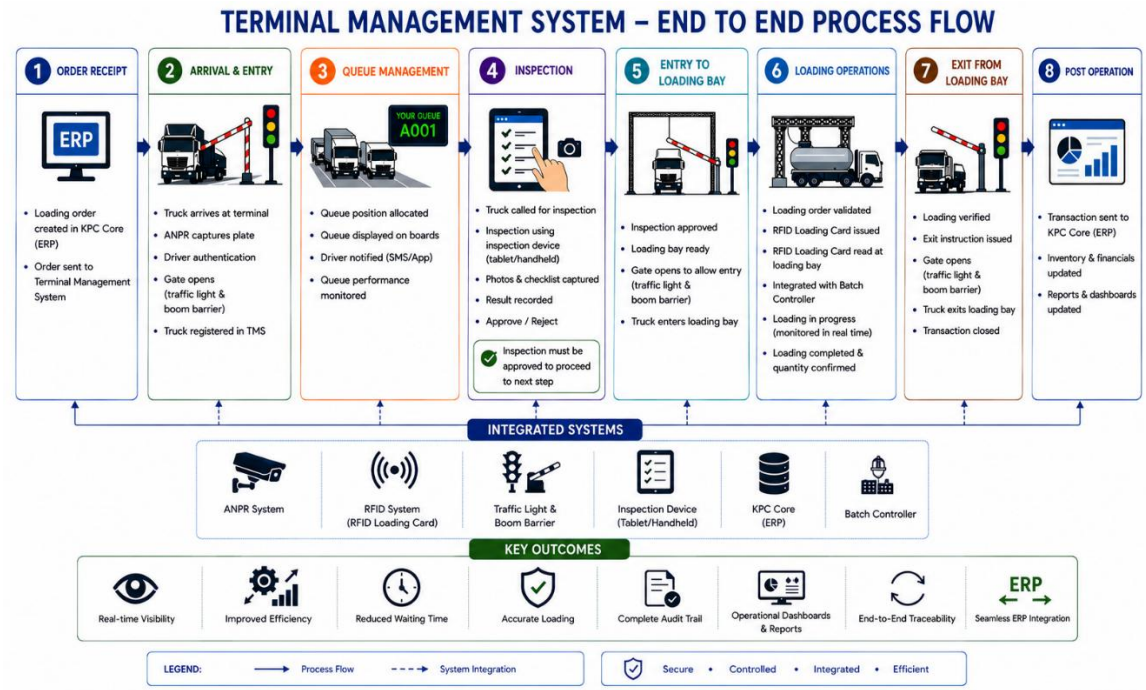
The PMO shall promote transparency, collaboration, accountability and timely communication among all stakeholders while maintaining independence in programme governance, reporting and assurance activities.

2.0.3 Desired Architecture

2.0.2.1 Enterprise Architecture



2.0.2.2 *TMS Architecture*



Notes:

i. The following hardware are not in the scope of this project; The ANPR Cameras, Boom barriers and traffic lights,

ii. This is a baseline Architecture the tenderers are invited to suggest improvements or align the same to their proposed solution without material deviation.
iii. Whereases the Architecture is comprehensive and covers many functions within KPC the scope of this project is limited to components identified in the BOM, Functional, Technical, Security, User, Availability, and Performance requirements together with Implementation Services required to deliver a Unified Enterprise Digital Solution.

LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES

The PMO shall act as KPC's independent programme management and assurance partner and shall safeguard KPC's interests by providing objective oversight of the Programme. The PMO shall ensure that the Programme is implemented in accordance with the approved scope, schedule, budget, quality requirements, governance framework, contractual obligations, implementation milestones and strategic business objectives.
The PMO shall work collaboratively with KPC, the Enterprise Digital Transformation Solution Contractor(s), Original Equipment Manufacturers (OEMs), implementation partners and other stakeholders while maintaining its independence in programme governance, reporting and quality assurance.

2.1.1 Objectives of LOT 1

2.1.1.1 *Overall Objective*

The overall objective of this assignment is to provide independent Programme Management Office (PMO) Services to support KPC in the successful planning, governance, coordination, monitoring, control and delivery of the Enterprise Digital Transformation Programme from contract mobilization through implementation, stabilization, benefits realization and programme closure.
The PMO shall establish effective programme governance, provide independent oversight of implementation activities, monitor contractor performance, facilitate informed decision-making and support KPC in achieving the Programme objectives within the approved scope, schedule, budget and quality requirements.

2.1.1.2 *Specific Objectives*

The PMO shall support KPC in achieving the following objectives.

No.	Objective
1	Establish, implement and maintain an effective Programme Governance Framework.
2	Coordinate all programme workstreams, implementation contractors, consultants and key stakeholders.
3	Develop, maintain and monitor the Integrated Master Programme Plan and programme baselines.
4	Monitor programme performance against approved scope, schedule, cost, quality and benefits realization targets.
5	Provide independent quality assurance across all implementation phases and contractual deliverables.
6	Establish and administer programme risk, issue, assumption, dependency and change management processes.
7	Monitor implementation contractor performance against contractual obligations, milestones, KPIs and Service Levels.
8	Support business transformation, organizational change management, stakeholder engagement and business readiness activities.
9	Monitor realization of approved business benefits and strategic outcomes.

10	Provide executive reporting, programme dashboards and decision support to KPC governance bodies.
11	Coordinate stage gate reviews and verify readiness for progression between implementation phases.
12	Support successful transition to operations, hypercare, operational handover and programme closure.

2.1.2 Scope of Services

The PMO shall provide comprehensive programme management and independent assurance services throughout the entire Programme lifecycle. The Services shall commence immediately upon contract award and continue until completion of all contractual obligations, including post-implementation stabilization, knowledge transfer and programme closure.
The scope of services shall include, but not be limited to, the activities described below.

No.	Service Area	Scope of Services
1	Programme Governance	Establish and administer the Programme Governance Framework, governance structures, committee Terms of Reference, governance calendar, decision-making processes, reporting structures and governance documentation.
2	Programme Planning	Develop, maintain and monitor the Integrated Master Programme Plan, programme schedule, critical path, milestones, resource plans, dependencies and implementation roadmap.
3	Programme Coordination	Coordinate programme workstreams, implementation contractors, OEMs, consultants, KPC project teams and all programme stakeholders.
4	Project Controls	Monitor programme scope, schedule, cost, quality, resources, risks, issues, assumptions, dependencies and programme performance against approved baselines.
5	Business Process Transformation	Support business process harmonization, process optimization, adoption of leading practices and alignment with the Programme objectives.
6	Risk, Issue and Change Management	Establish and maintain programme Risk Registers, RAID Registers, Issue Logs, Change Registers, Decision Registers and associated governance processes.
7	Contract and Vendor Performance Management	Monitor implementation contractor performance, contractual compliance, milestone achievement, Service Levels, deliverables and contractual obligations and provide independent performance assessments to KPC.
8	Quality Assurance	Independently review programme deliverables, solution designs, implementation activities, testing outcomes, migration readiness and compliance with contractual requirements.
9	Organizational Change Management	Monitor stakeholder engagement, communications, organizational readiness, business adoption, training effectiveness and change management activities.
10	Data Migration and Cutover Assurance	Review and monitor data migration strategies, migration readiness, reconciliation activities, cutover planning, rollback procedures and deployment readiness.
11	Benefits Realization	Develop and maintain the Benefits Realization Framework and monitor achievement of programme benefits, KPIs and strategic outcomes.

12	Knowledge Transfer	Monitor knowledge transfer activities and ensure sustainable transfer of technical and operational knowledge to KPC personnel.
13	Reporting and Executive Support	Prepare executive dashboards, governance reports, programme status reports, financial reports, performance reports, decision papers and management presentations.
14	Stage Gate Management	Coordinate formal stage gate reviews, readiness assessments, implementation approvals and progression through the Programme lifecycle.
15	Milestone Verification	Verify completion of contractual deliverables and provide recommendations to KPC regarding milestone achievement and payment certification.

2.1.3 Programme Lifecycle Support

The PMO shall provide programme management and assurance services throughout all implementation phases of the Enterprise Digital Transformation Programme.

No.	Programme Phase	PMO Responsibilities	Key Deliverables
1	Mobilization and Programme Initiation	Mobilize the PMO team, establish programme governance, prepare programme management documentation, develop the Integrated Master Programme Plan and coordinate programme initiation activities.	Programme Charter, Programme Governance Framework, Integrated Master Programme Plan, Programme Management Plan
2	Business Requirements and Solution Design	Monitor requirements validation, review solution designs, coordinate architecture reviews, manage programme risks and support design stage gate approvals.	Design Assurance Reports, Architecture Review Reports, Stage Gate Assessment Reports
3	Infrastructure Deployment	Monitor infrastructure implementation, review infrastructure readiness, coordinate technical assurance and monitor implementation progress.	Infrastructure Readiness Reports, Quality Assurance Reports
4	Solution Configuration and Development	Monitor configuration activities, oversee programme controls, coordinate implementation workstreams, monitor contractor performance and conduct quality reviews.	Quality Assurance Reports, Programme Performance Reports, Contractor Performance Reports
5	Integration	Monitor interface development, integration testing, dependency management and enterprise integration readiness.	Integration Readiness Reports, Integration Assurance Reports
6	Data Migration	Monitor migration planning, data quality, reconciliation activities, migration execution, rollback readiness and migration assurance.	Migration Assurance Reports, Data Reconciliation Reports
7	Testing	Coordinate governance of System Integration Testing (SIT), User Acceptance Testing (UAT),	Testing Assurance Reports, Stage Gate Assessment Reports

		performance testing, security testing, defect management and testing readiness.	
8	Go-Live and Hypercare	Conduct go-live readiness assessments, monitor deployment activities, oversee hypercare, monitor stabilization activities and coordinate executive reporting.	Go-Live Readiness Report, Hypercare Performance Reports, Stabilization Reports
9	Operational Handover and Programme Closure	Monitor operational handover, knowledge transfer, benefits realization, lessons learned and programme closure activities.	Programme Closure Report, Benefits Realization Report, Lessons Learned Report, Final Handover Report

2.1.4 Key Deliverables

The PMO shall prepare, maintain, update and submit all deliverables necessary for the successful governance, planning, execution, monitoring and closure of the Enterprise Digital Transformation Programme. Unless otherwise approved by KPC, all deliverables shall be submitted in editable electronic format and Portable Document Format (PDF).
The PMO shall, at a minimum, produce the following deliverables.

No.	Deliverable	Description	Timing
1	Programme Charter	Overall programme charter defining objectives, governance, scope and implementation approach.	Within fifteen (15) Business Days of Contract Commencement
2	Programme Governance Framework	Governance structure, committees, decision-making framework, reporting arrangements and governance calendar.	Within thirty (30) Business Days
3	Integrated Master Programme Plan	Consolidated implementation programme incorporating all Lots, workstreams, milestones, dependencies and critical path.	Within thirty (30) Business Days and updated monthly
4	Programme Management Plan	Overall programme management methodology, controls and execution approach.	Within thirty (30) Business Days
5	Stakeholder Engagement and Communication Plan	Stakeholder identification, engagement strategy and communication framework.	Within forty-five (45) Business Days
6	Risk Management Plan	Programme risk management methodology, risk appetite, escalation procedures and mitigation framework.	Within forty-five (45) Business Days
7	Integrated RAID Register	Consolidated Risks, Assumptions, Issues and Dependencies Register maintained throughout the Programme.	Updated weekly

8	Change Management Framework	Programme change governance, change control procedures and approval workflows.	Within sixty (60) Business Days
9	Quality Management Plan	Quality assurance methodology, quality reviews and compliance framework.	Within forty-five (45) Business Days
10	Benefits Realization Framework	Programme benefits, KPIs, measurement approach and realization tracking.	Within sixty (60) Business Days
11	Programme Dashboards	Executive dashboards covering programme health, milestones, risks, finances and contractor performance.	Monthly
12	Programme Status Reports	Consolidated programme progress reports.	Weekly and Monthly
13	Contractor Performance Reports	Independent assessment of implementation contractor performance against contractual obligations.	Monthly
14	Financial Progress Reports	Budget monitoring, expenditure, forecasts and variance analysis.	Monthly
15	Stage Gate Assessment Reports	Independent readiness assessments for progression between implementation phases.	At each Stage Gate
16	Go-Live Readiness Assessment	Readiness assessment prior to production deployment.	Prior to Go-Live
17	Hypercare Performance Report	Monitoring of stabilization activities and operational readiness.	During Hypercare
18	Benefits Realization Report	Measurement of programme benefits against approved KPIs.	Quarterly and at Programme Closure
19	Lessons Learned Report	Lessons learned and recommendations for continuous improvement.	At Programme Closure
20	Programme Closure Report	Final report confirming completion of all contractual obligations and programme close-out.	At Programme Completion

2.1.5 Programme Governance Framework

2.1.5.1 *General*

The PMO shall establish, implement, administer and continuously improve a comprehensive Programme Governance Framework to support effective decision-making, accountability, programme control, quality assurance and successful delivery of the Enterprise Digital Transformation Programme.

The Governance Framework shall provide clear reporting lines, decision-making authority, escalation procedures, accountability structures and governance processes throughout the Programme lifecycle.

2.1.5.2 *Governance Principles*

The Programme Governance Framework shall be founded upon the following principles.

1. Clear accountability and ownership.
2. Transparency and integrity.

3. Timely and evidence-based decision-making.
4. Independent programme assurance.
5. Effective stakeholder engagement.
6. Proactive risk and issue management.
7. Controlled change management.
8. Compliance with KPC governance policies and applicable regulatory requirements.
9. Alignment with the approved Programme objectives, implementation milestones and strategic outcomes.
10. Continuous improvement throughout the Programme lifecycle.

2.1.5.3 *Programme Governance Structure*

The PMO shall support the governance structure set out below and shall ensure that all governance bodies operate effectively throughout the Programme lifecycle.

No.	Governance Body	Primary Responsibilities	Meeting Frequency
1	Board of Directors / Board Committee (where applicable)	Strategic oversight, approval of major programme decisions, funding, strategic risks and programme outcomes.	As Required
2	Executive Management	Executive sponsorship, strategic direction, resolution of escalated matters and approval of major programme decisions.	Monthly
3	Programme Steering Committee	Overall programme governance, approval of stage gates, review of programme performance, strategic risks and key decisions.	Monthly
4	Programme Management Committee	Operational programme management, coordination of workstreams, monitoring of milestones, issues and dependencies.	Bi-weekly
5	Technical Review Committee	Review and approval of solution architecture, infrastructure, integrations, cybersecurity and technical standards.	Bi-weekly or As Required
6	Change Advisory Board (CAB)	Review and approval of programme change requests, impact assessments and implementation schedules.	As Required
7	Risk Review Committee	Review programme risks, mitigation plans, compliance risks and emerging threats.	Monthly
8	Project Working Groups	Detailed planning, execution, issue resolution and coordination of day-to-day implementation activities.	Weekly

2.1.5.4 *Governance Responsibilities*

The PMO shall facilitate the effective operation of all governance bodies and shall be responsible for the following activities.

1. Prepare governance calendars and meeting schedules.
2. Prepare meeting agendas and supporting documentation.
3. Coordinate attendance by all relevant stakeholders.
4. Facilitate governance meetings.
5. Record minutes, decisions and action items.
6. Maintain governance decision registers.
7. Monitor action item implementation and closure.
8. Monitor implementation of governance decisions.
9. Escalate unresolved issues through the approved governance structure.
10. Prepare governance reports and executive dashboards.
11. Maintain complete governance records throughout the Programme.

2.1.5.5 *Decision-Making Framework*

The PMO shall establish and maintain a Programme Decision Register documenting all strategic, technical, commercial and operational decisions.
Decision-making authority shall remain with KPC and shall be exercised through the appropriate governance bodies.

No.	Decision Type	Approval Authority
1	Programme Strategy and Objectives	Board of Directors / Executive Management
2	Programme Budget Revisions	Executive Management in accordance with KPC Delegation of Authority
3	Stage Gate Approvals	Programme Steering Committee
4	Solution Architecture	Technical Review Committee and KPC Technical Leads
5	Scope Changes	Programme Steering Committee upon recommendation of the Change Advisory Board
6	Programme Schedule Changes	Programme Steering Committee
7	Contract Variations	KPC in accordance with the Contract and Delegation of Authority
8	Operational Programme Decisions	Programme Management Committee
9	Day-to-Day Project Decisions	Project Managers within delegated authority

The PMO shall provide independent recommendations to KPC but shall not approve programme decisions on behalf of KPC.

2.1.5.6 *Escalation Framework*

The PMO shall establish and administer a structured escalation process to facilitate timely resolution of issues affecting successful programme delivery.
The escalation hierarchy shall be as follows.

Level	Escalation Authority
Level 1	Project Team / Workstream Leads
Level 2	Project Manager
Level 3	Programme Manager
Level 4	Programme Management Committee
Level 5	Programme Steering Committee
Level 6	Executive Management

Issues shall be escalated based on one or more of the following criteria.

1. Impact on programme schedule.
2. Impact on approved budget.
3. Impact on contractual milestones.
4. Impact on programme scope.
5. Impact on quality.
6. Business disruption.
7. Regulatory or statutory implications.
8. Cybersecurity risks.
9. Health, Safety, Security and Environmental (HSSE) risks.
10. Reputational impact.

2.1.5.7 *Reporting Requirements*

The PMO shall prepare and submit the reports listed below.

No.	Report	Frequency	Primary Audience
1	Weekly Progress Report	Weekly	Programme Management Committee
2	Monthly Programme Status Report	Monthly	Executive Management
3	Executive Dashboard	Monthly	Executive Management
4	Steering Committee Report	Monthly	Programme Steering Committee
5	Integrated RAID Register	Weekly	Programme Management Committee
6	Risk Register	Monthly or As Required	Risk Review Committee
7	Issue Register	Weekly	Programme Management Committee
8	Change Register	Monthly	Change Advisory Board
9	Financial Progress Report	Monthly	Executive Management
10	Contractor Performance Report	Monthly	Programme Steering Committee
11	Programme Health Assessment	Quarterly	Executive Management
12	Benefits Realization Report	Quarterly	Executive Management
13	Stage Gate Assessment Report	At each Stage Gate	Programme Steering Committee

2.1.5.8 *Stage Gate Reviews*

The PMO shall coordinate formal Stage Gate Reviews throughout the implementation lifecycle to verify readiness before progression to subsequent phases.

Each Stage Gate Review shall assess completion of required deliverables, achievement of implementation milestones, readiness of the next phase and outstanding programme risks.

Gate	Stage Gate	Primary Purpose
SG-1	Mobilization and Programme Initiation	Approval of Programme Charter, Governance Framework, Mobilization Plan and Integrated Master Programme Plan.
SG-2	Business Requirements and Solution Design	Approval of Business Requirements, Solution Design, Enterprise Architecture and implementation approach.
SG-3	Infrastructure Readiness	Confirmation that ICT infrastructure, environments and supporting platforms are ready for solution deployment.
SG-4	Solution Configuration and Development	Confirmation that solution configuration, custom developments and integrations are substantially complete.

Gate	Stage Gate	Primary Purpose
SG-5	Integration and Data Migration Readiness	Approval to commence final integration testing, migration and cutover activities.
SG-6	Testing Exit	Confirmation of successful completion of System Integration Testing, User Acceptance Testing, Performance Testing and Security Testing.
SG-7	Go-Live Readiness	Approval of production deployment following successful readiness assessment.
SG-8	Hypercare Exit	Confirmation that stabilization objectives have been achieved and transition to operational support may commence.
SG-9	Programme Closure	Confirmation of completion of contractual obligations, operational handover and programme closure.

Progression beyond any Stage Gate shall require formal approval by the appropriate governance authority.

2.1.5.9 *Governance Documentation*

The PMO shall establish, maintain and regularly update the following governance documentation.

No.	Governance Document
1	Programme Governance Framework
2	Governance Calendar
3	Committee Terms of Reference
4	Delegation of Authority Matrix
5	Decision Register
6	Integrated RAID Register
7	Risk Register
8	Issue Register
9	Action Register
10	Change Register
11	Stage Gate Approval Register
12	Programme Dashboard
13	Programme Performance Reports
14	Meeting Minutes and Action Logs

2.1.5.10 *Continuous Improvement*

The PMO shall periodically assess the effectiveness of the Programme Governance Framework and recommend improvements to governance processes, reporting mechanisms, decision-making structures, project controls and stakeholder engagement practices.

Recommendations shall be documented, presented to KPC and, where approved, incorporated into the Programme Governance Framework.

2.1.6 Staffing and Key Personnel Requirements

2.1.6.1 *General*

The Tenderer shall provide a multidisciplinary Programme Management Office (PMO) comprising suitably qualified, experienced and competent personnel necessary for the successful delivery of the Services described in this Tender.

The proposed team shall possess demonstrable experience in managing large-scale enterprise digital transformation programmes involving enterprise applications, ICT infrastructure, systems

integration, cybersecurity, organizational change management, business transformation and multi-vendor programme delivery.
The Tenderer shall ensure that all proposed Key Personnel remain available throughout the duration of the Programme unless otherwise approved in writing by KPC.

2.1.6.2 ***Core PMO Team***

The Tenderer shall provide, at a minimum, the Key Personnel specified below.

No.	Position	Minimum Quantity	Minimum Experience
1	Programme Director	1	15 Years
2	Programme Manager	1	12 Years
3	Deputy Programme Manager	1	10 Years
4	PMO Manager	1	10 Years
5	Planning and Project Controls Lead	1	10 Years
6	Risk and Quality Assurance Lead	1	10 Years
7	Commercial and Contract Management Lead	1	10 Years
8	Organizational Change Management and Communications Lead	1	10 Years
9	Benefits Realization Lead	1	8 Years
10	Business Process Transformation Lead	1	10 Years
11	Technical Assurance Lead	1	12 Years
12	Enterprise Architecture Advisor	1	12 Years
13	Data Migration Assurance Lead	1	10 Years
14	Testing and Cutover Assurance Lead	1	10 Years
15	Training and Knowledge Transfer Lead	1	8 Years
16	PMO Analysts	As Required	5 Years

The Tenderer may propose additional specialist resources where necessary to ensure successful delivery of the Programme.

2.1.6.3 ***Minimum Qualifications***

Unless otherwise approved by KPC, the proposed Key Personnel shall possess, at a minimum, the qualifications set out below or equivalent internationally recognised qualifications.

No.	Position	Minimum Qualification
1	Programme Director	Master's degree in information technology, Engineering, Computer Science, Business Administration, Project Management or a related discipline, together with a recognised programme management certification such as PgMP, MSP Practitioner, PRINCE2 Practitioner, PMP or equivalent. Excellent fluency in English
2	Programme Manager	Bachelor's Degree in a relevant discipline together with PMP, PRINCE2 Practitioner, MSP Practitioner or equivalent. Excellent fluency in English
3	PMO Manager	Bachelor's Degree in a relevant discipline together with recognised PMO or Project Management certification.
4	Technical Assurance Lead	Degree in Computer Science, Information Technology, Engineering or related discipline together with relevant enterprise technology certifications. Excellent fluency in English

5	Enterprise Architecture Advisor	Degree in a relevant discipline together with TOGAF or equivalent Enterprise Architecture certification.
6	Risk and Quality Assurance Lead	Degree in a relevant discipline together with recognised Risk Management and/or Quality Management certification.
7	Commercial and Contract Management Lead	Degree in Law, Procurement, Quantity Surveying, Commerce, Business Administration or related discipline together with recognised Contract Management certification.
8	Organizational Change Management Lead	Degree in Human Resource Management, Organizational Development, Business Administration, Psychology or related discipline together with recognised Change Management certification.
9	Other Specialists	Relevant academic and professional qualifications appropriate to the proposed role.

Equivalent internationally recognised qualifications and certifications shall be acceptable.

2.1.6.4 *General Experience Requirements*

All proposed Key Personnel shall:

1. Possess experience commensurate with their proposed responsibilities.
2. Demonstrate successful participation in enterprise-wide digital transformation programmes of similar scale and complexity.
3. Demonstrate experience in programme governance, stakeholder management and executive reporting.
4. Possess excellent communication, presentation and interpersonal skills.
5. Be proficient in written and spoken English.
6. Be available for the duration of the assignment.

Preference shall be given to personnel with demonstrable experience in:

a) Oil and gas.
b) Midstream petroleum operations.
c) Pipeline operations.
d) Critical National Infrastructure.
e) Energy utilities.
f) Large public sector organizations.
g) Multi-vendor ERP implementation programmes.
h) Enterprise Digital Transformation Programmes.

2.1.6.5 *Key Personnel Responsibilities*

The Tenderer shall submit detailed Terms of Reference for each proposed Key Person, including:

1. Roles and responsibilities.
2. Reporting relationships.
3. Decision-making authority.
4. Academic qualifications.
5. Professional certifications.
6. Relevant project experience.
7. Resource allocation to the Programme.
8. Expected duration of assignment.

2.1.6.6 *Personnel Availability*

Key Personnel proposed in the Bid shall be deemed committed to the Programme.

The Tenderer shall not replace any Key Person without the prior written approval of KPC except in circumstances beyond the Tenderer's reasonable control, including resignation, prolonged illness, incapacity or other exceptional circumstances.

2.1.6.7 ***Replacement of Key Personnel***

Where replacement of Key Personnel becomes necessary:

1. The Tenderer shall notify KPC in writing, stating the reasons for the proposed replacement.
2. The proposed replacement shall possess qualifications and experience equal to or better than those of the person being replaced.
3. KPC reserves the right to accept or reject the proposed replacement.
4. The Tenderer shall provide an adequate overlap and structured handover period to ensure continuity of the Services.
5. All costs associated with replacement of personnel shall be borne by the Tenderer.

2.1.6.8 ***Resource Mobilization***

The successful Tenderer shall mobilize the PMO team in accordance with the approved Mobilization Plan and Integrated Master Programme Plan.

The Tenderer shall ensure that appropriate specialist resources are deployed throughout each implementation phase to support the Programme lifecycle and achievement of contractual milestones.

2.1.6.9 ***Curriculum Vitae Requirements***

The Tenderer shall submit signed Curriculum Vitae (CVs) for all proposed Key Personnel.

Each Curriculum Vitae shall include, at a minimum:

1. Full Name.
2. Proposed Position.
3. Academic Qualifications.
4. Professional Certifications.
5. Professional Memberships, where applicable.
6. Employment History.
7. Relevant Project Experience.
8. Role in the proposed assignment.
9. Duration of involvement in referenced projects.
10. Declaration of availability.

Copies of academic certificates, professional certifications and other supporting documentation shall be submitted with the Proposal.

2.1.6.10 ***KPC's Right to Verify Personnel***

KPC reserves the right, during the evaluation process or at any time prior to Contract award, to:

1. Interview proposed Key Personnel.
2. Verify academic qualifications and professional certifications.
3. Verify employment history.
4. Conduct reference checks.
5. Validate claimed project experience.
6. Request clarification regarding proposed roles and responsibilities.
7. Reject any proposed Key Person who fails to satisfy the minimum requirements of this TENDER.
8. Require substitution of personnel who are unavailable or do not meet the stated requirements.

2.1.7 Deliverables and Reporting Requirements

2.1.7.1 *General*

The PMO shall prepare, maintain and submit all reports, registers, dashboards and programme documentation necessary for the effective governance, planning, monitoring, execution and successful completion of the Enterprise Digital Transformation Programme.

Unless otherwise approved by KPC, all deliverables shall be prepared in English and submitted in editable electronic formats including Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Project and Microsoft Visio together with Portable Document Format (PDF) versions.

All deliverables shall remain current throughout the Programme lifecycle and shall reflect the latest approved programme information.

2.1.7.2 *Programme Deliverables*

The PMO shall submit, at a minimum, the following deliverables.

No.	Deliverable	Timing	Review and Approval
1	Programme Charter	Within 15 Business Days of Contract Commencement	KPC
2	Programme Governance Framework	Within 30 Business Days	KPC
3	Integrated Master Programme Plan	Within 30 Business Days and updated monthly	KPC
4	Programme Management Plan	Within 30 Business Days	KPC
5	Stakeholder Engagement and Communication Plan	Within 45 Business Days	KPC
6	Risk Management Plan	Within 45 Business Days	KPC
7	Quality Management Plan	Within 45 Business Days	KPC
8	Benefits Realization Framework	Within 60 Business Days	KPC
9	Organizational Change Management Strategy	Within 60 Business Days	KPC
10	Knowledge Transfer Plan	Within 60 Business Days	KPC
11	Programme Closure Report	At Programme Completion	KPC

2.1.7.3 *Periodic Reporting Requirements*

The PMO shall prepare and submit the following reports throughout the Contract Period.

No.	Report	Frequency	Minimum Contents
1	Weekly Progress Report	Weekly	Progress against plan, completed activities, planned activities, issues requiring attention and upcoming milestones.
2	Monthly Programme Status Report	Monthly	Scope, schedule, budget, quality, risks, issues, dependencies, changes, milestone status and overall programme performance.
3	Executive Dashboard	Monthly	Executive summary, milestone status, financial performance, programme health, strategic risks and key decisions required.
4	Steering Committee Report	Monthly	Programme performance, milestone achievement, contractor performance, risks, issues and approvals required.
5	Integrated RAID Register	Weekly	Risks, assumptions, issues, dependencies and action status.

6	Financial Performance Report	Monthly	Budget utilization, expenditure, commitments, forecasts and variances.
7	Contractor Performance Report	Monthly	Performance against milestones, contractual obligations, KPIs, Service Levels and corrective actions.
8	Change Register	Monthly	Approved, pending and rejected Change Requests.
9	Benefits Realization Report	Quarterly	Progress against approved business benefits and strategic KPIs.
10	Stage Gate Assessment Report	At each Stage Gate	Readiness assessment, outstanding issues, recommendations and approval status.

2.1.7.4 *Executive Dashboards*

The PMO shall develop and maintain Executive Dashboards providing an accurate and current view of Programme performance.

At a minimum, the dashboards shall include:

1. Overall Programme Health (RAG Status).
2. Milestone Achievement.
3. Schedule Performance.
4. Budget Performance.
5. Risk Exposure.
6. Issue Status.
7. Change Request Status.
8. Contractor Performance.
9. Resource Utilization.
10. Benefits Realization Status.
11. Stage Gate Status.
12. Key Decisions Required.

Executive Dashboards shall be suitable for presentation to Executive Management and the Programme Steering Committee.

2.1.7.5 *Meeting Support*

The PMO shall coordinate and support all Programme Governance meetings.

The Services shall include:

1. Preparation of meeting agendas.
2. Distribution of supporting documentation.
3. Coordination of attendance.
4. Recording of attendance.
5. Preparation of meeting minutes.
6. Maintenance of Action Registers.
7. Maintenance of Decision Registers.
8. Monitoring closure of agreed actions.

Draft meeting minutes shall be circulated within five (5) Business Days after each meeting unless otherwise agreed by KPC.

2.1.7.6 *Programme Document Management*

The PMO shall establish and maintain a centralized Programme Document Management Repository.

The Repository shall:

1. Maintain structured document storage.
2. Maintain document version control.

3. Record document approvals.
4. Control user access.
5. Maintain complete audit trails.
6. Support collaboration among authorized stakeholders.
7. Preserve all Programme records throughout the Contract Period.

All Programme documentation shall remain the property of Kenya Pipeline Company PLC.

2.1.7.7 *Deliverable Review and Approval Process*

Unless otherwise specified in the Contract, all deliverables shall be reviewed and approved in accordance with the process set out below.

No.	Activity	Responsibility
1	Preparation of Deliverable	PMO
2	Internal Quality Review	PMO
3	Submission of Deliverable	PMO
4	Technical and Business Review	KPC
5	Consolidation of Review Comments	KPC
6	Revision and Resubmission	PMO
7	Verification of Revisions	KPC
8	Final Approval	KPC

KPC shall review submitted deliverables within the agreed review period and communicate comments to the PMO.

The PMO shall address all review comments and resubmit revised deliverables for approval.

2.1.7.8 *Deliverable Acceptance Criteria*

Unless otherwise specified, each deliverable shall satisfy the minimum acceptance criteria set out below.

No.	Requirement	Acceptance Criteria
1	Completeness	All required sections, appendices and supporting documentation have been submitted.
2	Accuracy	Information is complete, accurate, validated and internally consistent.
3	Compliance	Deliverable complies with this TENDER, the Contract, approved methodologies, applicable standards and Programme Governance Framework.
4	Quality	Deliverable meets agreed quality standards and has undergone internal quality assurance.
5	Timeliness	Deliverable has been submitted within the approved programme schedule.
6	Review Comments	All KPC review comments have been satisfactorily addressed.
7	Format	Deliverable has been submitted in the required editable and PDF formats.
8	Approval	Deliverable has received formal written approval from the designated KPC Representative.

Acceptance of any deliverable shall not relieve the PMO of responsibility for defects, omissions, inaccuracies or non-conformities subsequently identified during the Programme.

2.1.7.9 *Records Management and Retention*

The PMO shall establish and maintain comprehensive Programme records throughout the Contract Period.

Programme records shall include, but not be limited to:

i. Programme reports.
ii. Governance documentation.
iii. Registers.
iv. Correspondence.
v. Meeting minutes.
vi. Programme schedules.
vii. Financial reports.
viii. Contractor performance reports.
ix. Stage Gate documentation.
x. Supporting evidence for milestone certification.

Upon completion or termination of the Contract, all Programme records shall be handed over to KPC in an organized and searchable format.

2.1.7.10 *Continuous Improvement*

The PMO shall periodically review reporting requirements, governance processes and document management practices and recommend improvements to enhance programme visibility, decision-making, efficiency and governance effectiveness.

Implementation of approved improvements shall be incorporated into the Programme Governance Framework and associated management plans.

2.1.8 Service Levels and Key Performance Indicators (KPIs)

2.1.8.1 *General*

The PMO shall perform the Services in accordance with the Service Levels and Key Performance Indicators (KPIs) specified in this Section.

The KPIs shall be used by KPC to assess the effectiveness of the PMO in delivering programme governance, programme management, reporting, quality assurance, contractor oversight and advisory services throughout the Contract Period.

Performance shall be reviewed periodically and shall form part of the PMO's overall performance evaluation.

Failure to consistently achieve the agreed Service Levels may require implementation of corrective actions and may constitute grounds for contractual remedies in accordance with the Conditions of Contract.

2.1.8.2 *Service Level Principles*

The PMO shall ensure that:

i. Programme information is accurate, complete and submitted within agreed timelines.
ii. Risks, issues and dependencies are proactively identified, monitored and managed.
iii. Governance meetings are effectively coordinated and documented.
iv. Executive reporting supports timely and informed decision-making.
v. Programme controls are consistently applied across all workstreams.
vi. Quality assurance activities are undertaken in accordance with the approved Quality Management Plan.
vii. Programme deliverables are submitted in accordance with the approved Programme Schedule.
viii. Stage Gate Reviews are completed before progression to subsequent implementation phases.
ix. Contractor performance is independently monitored and objectively reported.

x. Programme benefits are continuously monitored against approved KPIs.

2.1.8.3 ***Key Performance Indicators***

No.	KPI Reference	Key Performance Indicator	Performance Target	Measurement Frequency
1	KPI-01	Timely submission of scheduled reports	≥95% submitted on or before the due date	Monthly
2	KPI-02	Accuracy of Programme milestone reporting	100% of approved milestones monitored and reported	Monthly
3	KPI-03	Governance meeting support	100% of scheduled governance meetings supported	Monthly
4	KPI-04	Distribution of meeting minutes	Draft minutes issued within five (5) Business Days	Monthly
5	KPI-05	Action Register management	≥95% of actions monitored and updated within agreed timelines	Monthly
6	KPI-06	RAID Register maintenance	Updated before each governance meeting	Weekly
7	KPI-07	Executive Dashboard submission	Submitted within agreed reporting timelines	Monthly
8	KPI-08	Quality assurance reviews	100% completed in accordance with the approved Quality Management Plan	Monthly
9	KPI-09	Stage Gate Reviews	100% completed before approval of subsequent implementation phases	As Required
10	KPI-10	Benefits Realization reporting	Submitted in accordance with the approved Benefits Realization Framework	Quarterly

2.1.8.4 ***Programme Governance and Risk Management KPIs***

No.	KPI Reference	Key Performance Indicator	Performance Target
1	KPI-11	Programme risks reviewed	100% reviewed within the agreed reporting cycle
2	KPI-12	High-risk issues escalated	Within two (2) Business Days of identification
3	KPI-13	Critical issues escalated	Within one (1) Business Day of identification
4	KPI-14	Risk mitigation actions monitored	≥95% tracked against agreed completion dates
5	KPI-15	Change Requests processed	100% processed in accordance with the approved Change Management Process
6	KPI-16	Milestone verification completed	100% completed before payment certification
7	KPI-17	Contractor performance reviews completed	100% completed within the agreed reporting cycle
8	KPI-18	Programme Health Assessment	Submitted within agreed reporting timelines

2.1.8.5 *Reporting Quality Requirements*

All reports prepared by the PMO shall:

i. Be accurate and evidence based.
ii. Be complete and free from material errors.
iii. Be submitted within agreed reporting timelines.
iv. Utilize approved templates and formats.
v. Be supported by current programme data.
vi. Clearly identify programme risks, issues, dependencies and recommended actions.
vii. Clearly identify decisions required from Programme Governance Bodies.
viii. Include analysis of progress against approved implementation milestones.

KPC reserves the right to reject reports that fail to satisfy these requirements.

2.1.8.6 *Contractor Performance Monitoring*

The PMO shall independently monitor implementation contractor performance throughout the Programme.

Performance monitoring shall include, but not be limited to:

i. Delivery of contractual milestones.
ii. Progress against the Integrated Master Programme Plan.
iii. Quality of contractual deliverables.
iv. Resolution of defects and non-conformities.
v. Compliance with Service Levels.
vi. Resource deployment.
vii. Contractual compliance.
viii. Risk exposure.
ix. Health, Safety, Security and Environmental compliance where applicable.
x. Overall implementation performance.

The PMO shall provide objective assessments and recommendations but shall not direct implementation contractors outside the authority delegated by KPC.

2.1.8.7 *Performance Review Meetings*

Formal PMO Performance Review Meetings shall be held at least quarterly.

The reviews shall assess:

1. Achievement of KPIs.
2. Programme governance effectiveness.
3. Status of contractual deliverables.
4. Quality of programme reporting.
5. Contractor oversight effectiveness.
6. Risk management performance.
7. Resource adequacy.
8. Progress against implementation milestones.
9. Opportunities for continuous improvement.

Where performance deficiencies are identified, KPC may require the PMO to prepare and implement a Performance Improvement Plan.

2.1.8.8 *Performance Measurement Methodology*

Performance against the agreed KPIs shall be measured using objective evidence including:

1. Approved Programme Reports.
2. Executive Dashboards.
3. Governance Records.
4. Meeting Minutes.

5. Programme Schedules.
6. Stage Gate Assessment Reports.
7. Milestone Verification Reports.
8. Deliverable Acceptance Records.
9. Audit Reports.
10. Contractor Performance Reports.
11. Programme Health Assessments.

KPC reserves the right to verify reported performance through audits, independent reviews or other verification activities.

2.1.8.9 *Continuous Improvement*

The PMO shall continuously identify opportunities to improve programme governance, reporting, project controls, programme performance and stakeholder engagement.
Recommendations shall be documented, prioritized and presented to KPC for approval.

2.1.8.10 *Corrective Action*

Where agreed Service Levels or KPI targets are not achieved, the PMO shall:

i. Identify the root cause of the performance shortfall.
ii. Prepare a Corrective Action Plan.
iii. Submit the Corrective Action Plan to KPC within ten (10) Business Days.
iv. Implement the approved corrective actions.
v. Monitor implementation of the corrective actions.
vi. Report progress until the performance issue has been fully resolved.

Repeated failure to achieve agreed Service Levels or KPI targets may constitute a material breach of Contract and may result in the application of contractual remedies in accordance with the Conditions of Contract.

2.1.9 Acceptance Criteria

2.1.9.1 *General*

All Services and deliverables provided by the PMO shall be subject to review, verification and formal acceptance by Kenya Pipeline Company PLC (KPC).
Acceptance shall confirm that the Services and deliverables comply with the requirements of this TENDER, the Contract, the approved Programme Governance Framework, applicable standards and agreed acceptance criteria.
Acceptance of any deliverable or milestone shall not relieve the PMO of its responsibility to correct any errors, omissions, defects or non-conformities identified during the Programme lifecycle.

2.1.9.2 *Acceptance Principles*

Acceptance shall be based on the following principles:

i. Compliance with the requirements of the Contract and this TENDER.
ii. Completion of all agreed activities.
iii. Compliance with approved methodologies, templates and standards.
iv. Accuracy, completeness and internal consistency.
v. Fitness for the intended purpose.
vi. Incorporation of all KPC review comments.
vii. Formal written approval by the designated KPC Representative.
viii. Successful completion of the applicable Stage Gate Review.
ix. Achievement of the associated implementation milestone.

2.1.9.3 *Deliverable Review and Acceptance Process*

The review and acceptance process shall comprise the following stages.

No.	Activity	Responsibility
1	Preparation and Internal Quality Review	PMO
2	Submission of Deliverable	PMO
3	Technical and Business Review	KPC
4	Consolidation of Review Comments	KPC
5	Revision and Resubmission	PMO
6	Verification of Revisions	KPC
7	Formal Acceptance	KPC

KPC shall communicate review comments within the agreed review period.

The PMO shall address all comments before resubmitting the deliverable for final approval.

2.1.9.4 *Deliverable Acceptance Criteria*

Unless otherwise agreed, each deliverable shall satisfy the following minimum acceptance criteria.

No.	Requirement	Acceptance Criteria
1	Completeness	All required sections, appendices, schedules and supporting documentation have been submitted.
2	Accuracy	Information is accurate, validated and internally consistent.
3	Compliance	Deliverable complies with the Contract, this TENDER, approved methodologies and Programme Governance Framework.
4	Quality	Deliverable satisfies agreed quality standards and has successfully completed internal quality assurance.
5	Timeliness	Submitted within the approved Programme Schedule.
6	Review Comments	All review comments have been satisfactorily addressed.
7	Format	Submitted in editable electronic format together with PDF unless otherwise approved.
8	Approval	Approved in writing by the designated KPC Representative.

2.1.9.5 *Service Acceptance*

In addition to document deliverables, PMO Services shall be assessed against the following criteria.

i. Achievement of approved implementation milestones.
ii. Delivery of contractual responsibilities.
iii. Compliance with agreed Service Levels and KPIs.
iv. Effectiveness of Programme Governance.
v. Quality and timeliness of executive reporting.
vi. Timeliness of issue escalation.
vii. Effectiveness of stakeholder engagement.
viii. Responsiveness to KPC requests.
ix. Quality of contractor oversight.
x. Overall contribution to successful delivery of the Enterprise Digital Transformation Programme.

2.1.9.6 *Non-Conforming Deliverables*

Where a deliverable fails to satisfy the acceptance criteria, KPC may:

i. Reject the deliverable.
ii. Request clarification.
iii. Require revision and resubmission.
iv. Request additional supporting documentation.
v. Require additional quality assurance activities.

vi. Withhold acceptance until all deficiencies have been satisfactorily addressed.

The PMO shall correct all deficiencies at no additional cost to KPC.

2.1.9.7 *Resubmission*

Rejected deliverables shall be revised and resubmitted within the period specified by KPC.

Repeated submission of materially deficient deliverables may be treated as a performance issue and managed in accordance with the Conditions of Contract.

2.1.9.8 *Stage Gate Acceptance*

Formal acceptance shall be required at each Stage Gate before progression to the subsequent implementation phase.

Stage Gate Acceptance shall confirm that:

i. All planned activities for the phase have been completed.
ii. All mandatory deliverables have been approved.
iii. Outstanding risks have been reviewed and accepted by the appropriate governance body.
iv. Critical issues have been resolved or approved mitigation measures have been implemented.
v. Dependencies for the subsequent phase have been addressed.
vi. The Programme Steering Committee has approved progression to the next implementation phase.

2.1.9.9 *Final Acceptance*

Final Acceptance of the PMO Services shall occur upon:

1. Completion of all contractual obligations.
2. Approval of the Programme Closure Report.
3. Submission of all final reports, registers and supporting documentation.
4. Completion of knowledge transfer activities.
5. Handover of all Programme documentation and intellectual property to KPC.
6. Completion of Benefits Realization reporting as required under the Contract.
7. Resolution of all outstanding contractual obligations.

Final Acceptance shall not prejudice KPC's rights in respect of latent defects, breach of Contract or surviving contractual obligations.

2.1.9.10 *Acceptance Certificate*

Upon satisfactory completion of each contractual milestone, KPC shall issue a written Acceptance Certificate.

The Acceptance Certificate shall include:

1. Milestone reference.
2. Deliverable reference.
3. Date of acceptance.
4. Confirmation that acceptance criteria have been satisfied.
5. Outstanding observations, where applicable.
6. Name and designation of the approving KPC Representative.

Issuance of an Acceptance Certificate shall constitute the basis for certification of the corresponding payment milestone in accordance with Section **5.12** of this TENDER.

2.1.10 Performance-Based Payment Milestones

2.1.10.1 *General*

Payments under the PMO Contract shall be milestone-based and shall be made upon successful completion and formal acceptance of the corresponding Services and deliverables by KPC.

Each milestone payment shall be subject to:

1. Completion of all activities associated with the milestone.
2. Submission of all required deliverables.
3. Successful completion of the applicable Stage Gate Review.
4. Formal acceptance by KPC in accordance with Section **5.11**.
5. Submission of a valid invoice together with all required supporting documentation.
6. Compliance with all contractual obligations.

Certification of a payment milestone shall not constitute Final Acceptance of the Services.

2.1.10.2 ***Supporting Documentation***

Each application for payment shall include, where applicable:

1. Milestone Completion Report.
2. Deliverables associated with the milestone.
3. Acceptance Certificate issued by KPC.
4. Stage Gate Approval Record.
5. Updated Executive Dashboard.
6. Updated Integrated Master Programme Plan.
7. Updated RAID Register.
8. Financial Progress Report.
9. Contractor Performance Report.
10. Valid Tax Invoice.
11. Any other supporting documentation reasonably required by KPC.

2.1.10.3 ***Milestone Verification***

Prior to certification of any payment milestone, KPC shall verify that:

1. All milestone deliverables have been submitted.
2. Deliverables have been formally accepted.
3. The applicable Stage Gate has been successfully completed.
4. Programme KPIs have been satisfactorily achieved.
5. Contractor performance has been independently verified by the PMO.
6. Previously identified deficiencies have been satisfactorily resolved.

KPC reserves the right to defer certification where the applicable acceptance requirements have not been fully satisfied.

2.1.10.4 ***Deferred Payments***

Where a milestone has only been partially achieved, KPC may:

1. Defer payment until the milestone has been satisfactorily completed.
2. Certify payment only for the completed and accepted portion of the milestone where such portion is separable and provides value to KPC.
3. Require the PMO to rectify identified deficiencies prior to release of any outstanding payment.

2.1.10.5 ***Contract Variations***

Where KPC approves changes to the Programme that materially affect the PMO Services, the Parties may revise:

1. Payment milestones.
2. Milestone values.
3. Deliverables.
4. Implementation schedule.
5. Resource requirements.

All such revisions shall be effected through a formal Contract Variation.

2.1.10.6 *Retention*

KPC may retain **ten percent (10%) of each certified milestone payment** up to a maximum cumulative retention of **ten percent (10%) of the Contract Price**.

The retained amount shall be released upon:

1. Final Acceptance of the Services;
2. Completion of all contractual obligations;
3. Completion of knowledge transfer; and
4. Resolution of all outstanding defects, deficiencies and other contractual obligations.

Where permitted under the Contract, KPC may accept an equivalent **Performance Security** in lieu of retention, subject to the terms and conditions stipulated in the Contract.

2.1.10.7 *Taxes and Statutory Deductions*

All payments shall be subject to applicable taxes, statutory deductions and withholding obligations in accordance with the Laws of Kenya.

The Tenderer shall clearly identify all applicable taxes in the Financial Proposal.

2.1.10.8 *Final Payment*

Final Payment shall only be made upon:

1. Final Acceptance of the PMO Services.
2. Approval of the Programme Closure Report.
3. Completion of all contractual obligations.
4. Handover of all Programme documentation and records.
5. Submission of the Final Invoice.
6. Resolution of all outstanding contractual matters.

2.1.10.9 *Payment Terms*

Certified invoices shall be processed in accordance with the payment provisions specified in the Conditions of Contract.

No payment shall be made unless the applicable milestone has been successfully completed, formally accepted and certified by KPC.

LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION

2.2.1 Introduction

Kenya Pipeline Company PLC (KPC) intends to implement an integrated Enterprise Digital Transformation Solution to modernize its business processes, enterprise applications, operational systems, data capabilities and ICT infrastructure, while enhancing operational efficiency, business visibility, regulatory compliance, cybersecurity, resilience and long-term digital capability.

Lot 2 shall comprise the design, supply, implementation, configuration, integration, testing, commissioning, training, data migration, knowledge transfer, support and maintenance of the Enterprise Digital Transformation Solution and all associated components and professional services.

The Solution shall provide an integrated digital environment supporting KPC's corporate functions, commercial operations, pipeline and terminal operations, enterprise asset management, stakeholder engagement, Enterprise Data Analytics and AI, enterprise integration, cybersecurity integration, ICT infrastructure and operational technology integration.

The Contractor shall assume end-to-end responsibility for the complete solution, including all proposed software products, licences, infrastructure, interfaces, integrations, custom developments, configurations, migrations, professional services, training, documentation, warranties and support, whether delivered directly or through OEMs, consortium members, subcontractors, affiliates or other third parties.

The Solution shall be designed to support KPC's current operational requirements while providing scalability, interoperability, high availability, security and flexibility to accommodate future business growth, technology evolution and additional digital capabilities.

The Contractor shall implement the approved requirements by translating it into detailed To-Be business processes, workflows, configurations, system requirements and standard operating procedures. Any material deviation from the approved requirements shall require prior review and approval in accordance with KPC's established governance and change control arrangements.

Notably the contractor shall ensure that all the automated processes that are not redundant are migrated to the new platform. The tenderer must therefore include these processes in their scope and referrer to the landscape of the existing landscape listed in section 2.0.8 of this tender document.

2.2.2 Objectives of LOT 2

The objectives of Lot 2 are to provide KPC with a secure, integrated, scalable and sustainable Enterprise Digital Solution that enables the Company to modernize its business and operational processes and improve service delivery, operational efficiency and decision-making.

The Solution shall:

a) Replace and modernize identified legacy enterprise applications and technologies, including the existing SAP ECC6 and associated legacy platforms within the approved scope;
b) Provide an integrated enterprise business platform supporting KPC's corporate, financial, procurement, human resource, commercial, asset management, project management, risk, compliance and other business functions;
c) Provide integrated Mid-Stream Oil Operations and Terminal Management capabilities supporting KPC's pipeline, terminal, depot, truck loading and related operational processes;
d) Establish an Enterprise Data Analytics platform supporting data integration, data quality, data warehousing and/or data lake capabilities, master data management, business intelligence, enterprise reporting, advanced and predictive analytics, artificial intelligence,

machine learning, and AI-enabled decision support, while leveraging KPC's existing Power BI platform for visualization, dashboards, and self-service analytics;

e) Establish a robust Enterprise Integration and Development Platform capable of integrating KPC's enterprise applications, operational technology, external systems, government and regulatory platforms, financial institutions, customers, suppliers and other relevant third-party systems;
f) Integrate the Solution with KPC's existing cybersecurity capabilities, including Identity and Access Management (IAM), Privileged Access Management (PAM), Security Information and Event Management (SIEM) and other applicable security platforms;
g) Provide resilient and enterprise-grade ICT infrastructure, including compute, storage, virtualization, containerization, databases, high availability, disaster recovery and platform monitoring capabilities;
h) Enable integration between Information Technology (IT) and Operational Technology (OT) environments while maintaining appropriate security, segregation, monitoring and access controls;
i) Migrate relevant data from existing and legacy systems into the new Solution in a controlled, secure and validated manner, including data cleansing, mapping, transformation, reconciliation and validation;
j) Provide configurable workflows, automation, self-service and digital channels to improve business process efficiency and user experience;
k) Provide comprehensive auditability, segregation of duties, access controls, security logging and regulatory compliance capabilities;
l) Provide a scalable architecture capable of supporting KPC's current and future business requirements without requiring major architectural redesign;
m) Establish appropriate business continuity, high availability and disaster recovery capabilities for critical systems and workloads;
n) Provide structured training, knowledge transfer, documentation and capacity building to enable KPC personnel to operate, administer, support and sustain the Solution;
o) Provide comprehensive warranty, post-implementation support and maintenance services to ensure continued availability, performance, security and reliability of the Solution; and
p) Provide a foundation for continuous digital innovation, including mobile capabilities, workflow automation, analytics, artificial intelligence and other emerging technologies where applicable and approved by KPC.

2.2.3 Scope of the Enterprise Digital Transformation Solution

The Contractor shall provide an integrated Enterprise Digital Transformation Solution comprising all software, hardware, infrastructure, licences, subscriptions, configurations, integrations, interfaces, custom developments, data migration, implementation services, training, documentation, warranty, support and maintenance necessary to deliver a complete and operational solution for KPC.

The scope shall include, but shall not be limited to, the following solution components.

2.2.3.1 *Corporate Services*

The Solution shall provide integrated corporate business capabilities covering Strategic Planning and Performance Management, Enterprise Risk Management, Financial Operations and Accounting, Budget Management, Treasury, Supply Chain Management, Contract Lifecycle Management, Human Resource and Payroll, Safety Management, Project Lifecycle Management and other approved corporate business processes.

2.2.3.2 *Sales and Commercial Management*

The Solution shall provide capabilities for Order Management, Customer Account Management, Billing and Revenue Management, Pricing Management, Commercial Contract Management, Revenue Forecasting and other relevant commercial business processes.

2.2.3.3 ***Stakeholder Management***

The Solution shall provide stakeholder-facing and engagement capabilities covering Customer Relationship Management, Supplier Relationship Management, Marketing and Campaign Management, Communications Management, Complaint Management, customer and supplier portals and other approved stakeholder engagement services.

2.2.3.4 ***Enterprise Asset Management***

The Solution shall provide integrated Enterprise Asset Management capabilities covering Maintenance Management, Asset Integrity Management, Work Management, Field Service Management, Maintenance Inventory, Reliability Management and Asset Performance Management.

2.2.3.5 ***Cross-Cutting Enterprise Services***

The Solution shall provide shared enterprise services supporting the business applications and operational platforms, including IT Service Management (ITSM), Enterprise Monitoring and Response Platform, enterprise workflow services and other reusable enterprise capabilities.

2.2.3.6 ***Mid-Stream Oil Operations System (MSOOS)***

The Solution shall provide an integrated Mid-Stream Oil Operations System supporting KPC's petroleum pipeline and midstream operations, including Pipeline Planning and Scheduling, Marine Operations, Hydrocarbon Management, Customer Management, Quality Control Management, Pricing and Billing Management, Quantity Conversion Management, Inventory Management, Order-to-Cash processes and other relevant midstream petroleum operations.

2.2.3.7 ***Terminal Management System (TMS)***

The Solution shall provide an integrated Terminal Management System supporting efficient, secure and automated truck loading and terminal operations. KPC PLC handles hydrocarbons. All supplied equipment must comply with oil and gas industry standards including ATEX rating. The contractor must comply with all KPC safety practices.

The TMS shall include Queue Management for trucks and orders, truck and driver identification and verification, queue display boards, safety checklists, loading bay allocation, loading automation and integration with other loading operational systems.

The TMS shall support the streamlining of truck movement and loading operations at KPC terminals and depots to improve operational efficiency, safety, throughput, visibility and customer service.

2.2.3.8 ***Enterprise Data Analytics and AI***

The Solution shall provide an Enterprise Data Analytics and AI Platform comprising Enterprise data warehouse and/or data lake capabilities for raw, curated, and analytical data, data integration services, data cleansing, transformation, mapping and standardisation, data quality and governance, Business Intelligence, enterprise reporting, advanced and predictive analytics, Artificial Intelligence, Machine Learning, Generative AI, and AI-enabled decision support.

2.2.3.9 ***Enterprise and External Systems Integration***

The Solution shall provide an Enterprise Integration Platform supporting API development and management, API Developer Portal, Enterprise Service Bus (ESB), middleware, Service Mesh, event streaming, workflow integration, data synchronisation, OT integration, integration development tools and reusable integration services.

The Contractor shall design, develop, implement, test and support integrations between the Solution and KPC's existing and future enterprise applications, operational technology systems, banking systems, payment gateways, government and regulatory agencies, tax systems, identity providers, customer and supplier platforms, third-party applications, approved cloud services and other internal and external systems.

Integrations shall use appropriate industry-standard APIs, messaging services, data exchange mechanisms and integration protocols.
The scope shall include, where applicable, integration with government and regulatory platforms including KRA and other relevant agencies, banking and payment platforms, identity providers, customer and supplier platforms and other approved external systems.

2.2.3.10 ***Cybersecurity Integration***

The Solution shall integrate with KPC's existing cybersecurity ecosystem, including Identity and Access Management (IAM), Privileged Access Management (PAM), Security Information and Event Management (SIEM), endpoint security, security monitoring, privileged access controls, audit logging, identity federation, vulnerability management and security operations capabilities.

2.2.3.11 ***Infrastructure***

The Contractor shall provide the required enterprise ICT infrastructure for the Primary Data Centre and Disaster Recovery environment, including compute, storage, virtualization, container orchestration, databases, operating systems, high availability, load balancing, observability, platform monitoring, infrastructure management and other supporting digital platforms.
All infrastructure shall be appropriately sized and configured to support the proposed Solution, including its production, non-production, disaster recovery, integration, data and analytics workloads.

2.2.3.12 ***Operational Technology Integration***

The Solution shall support secure integration with KPC's operational technology environment, including SCADA systems, Terminal Automation Systems, Hydrant Management Systems, OT/IT firewalls, OT historians, Operational Data Repositories, Automatic Tank Gauging (ATG), Laboratory Information Management Systems (LIMS), Pipeline Integrity Management Systems (PIMS) and other applicable operational technology platforms.

2.2.3.13 ***Data Migration and Legacy System Transition***

The Contractor shall undertake the migration and transition of approved data, configurations, interfaces, historical information and other relevant information from KPC's existing and legacy systems into the new Solution.
The scope shall include data profiling, extraction, cleansing, transformation, mapping, validation, reconciliation, migration testing, cutover, post-migration validation and support.
The migration scope shall include the existing SAP ECC6 environment and other identified legacy applications and platforms within the approved project scope.

2.2.3.14 ***Professional Implementation Services***

The Contractor shall provide all professional services required for successful implementation of the Solution, including solution architecture, business process translation, detailed design, configuration, customisation, software development, systems integration, infrastructure deployment, testing, performance optimisation, data migration, training, documentation, knowledge transfer, commissioning, cutover, hyper care, warranty and post-implementation support.

In establishing their implementation effort, the tenderer shall refer to the information listed in solution sizing metrics in section 2.2.6.2 Solution Sizing Information. The tenderer must implement all the solutions in scope to meet all the functional, technical, security requirements.

2.2.3.15 ***Scope of Implementation***

This section defines the scope of the professional implementation services that the Contractor shall deliver for every solution component within Lot 2. It is written so that a tenderer can build a complete, bottom-up estimate of implementation effort from countable units of work, priced against the Work Breakdown Structure (WBS) in the Implementation Services BOM, and reconciled to the Solution Sizing Information in section 2.2.6.2.

Text highlighted in yellow identifies information that is to be provided by KPC before the tender is issued, or that the tenderer is required to declare in its response. A consolidated schedule of these items is given in section 2.2.2.15.9.

2.2.2.15.1 Purpose and Use of this Section

The tenderer shall use this section as follows:

i. Every WBS line in the Implementation Services BOM shall be quantified using the unit of measure and the quantity basis stated in section 2.2.2.15.5. Where a quantity is stated in this section or in section 2.2.6.2, the tenderer shall use it. Where a quantity is highlighted for KPC to provide, the tenderer shall use the value supplied by addendum. Where a quantity is highlighted for the tenderer to declare, the tenderer shall state its assumed value and the basis for it.

ii. Effort shall be stated in person-days per WBS line, together with the resource categories applied and the onsite/offsite split. Lump-sum effort without a unit basis will be treated as non-compliant with section 2.2.5.7.

iii. The scope described here is the implementation of the functional, technical, security and non-functional requirements of sections 2.2.4 in full. This section does not reduce, qualify or replace any requirement stated elsewhere in the tender document.

iv. The tenderer shall implement all automated processes in the existing landscape that are not redundant, as required in section 2.2.1, and shall include the effort for their re-implementation on the new platforms within the units below.

v. Any assumption the tenderer relies on that is not stated in this section shall be declared in the format required by section 2.2.2.15.8. Undeclared assumptions shall not be admitted as grounds for variation after award.

2.2.2.15.2 Basis of Estimate Principles

The following principles govern the scope and shall be reflected in the tenderer's effort estimate:

i. Standard functionality first. The Contractor shall meet requirements through configuration of standard product capability wherever the product provides it. Custom development is admissible only for a documented gap approved through the fit-gap process, and shall be built using the product's supported extension framework so that upgradeability is preserved.

ii. One integrated programme. The ERP and EAM platform, the electronic procurement service, the Mid-Stream Oil Operations System (MSOOS), the Terminal Management System (TMS), the analytics platform, the integration platform and the infrastructure are delivered as one solution under one Contractor, with one design authority, one integrated schedule, one test regime and one cutover plan per release.

iii. Deployment model. The ERP and EAM platform, MSOOS, TMS, analytics, integration and cross-cutting services are deployed on KPC infrastructure at the Primary Data Centre with disaster recovery at the DR site. If the electronic procurement service is a cloud-hosted subscription service; its implementation effort covers tenant provisioning, configuration, integration and supplier enablement, and no KPC-hosted infrastructure is required for it.

iv. Existing Visualization platform (Microsoft Power BI) . The existing enterprise visualisation platform may be retained for dashboards and self-service analytics; the analytics implementation delivers the data platform, models and content that feed it. However, the bidder is free to provide an alternative.

v. Sites and operations. The solution serves the sites listed under sizing reference A2 and operates on a 24/7 basis under the shift pattern in reference A5. Effort for site deployment, site testing and site training shall be estimated per site, not per programme.

vi. Legacy continuity. The existing ERP platform continues to operate on the new infrastructure until each of its functions is cut over to the new solution, and thereafter in read-only mode for the retention period stated in section 2.2.2.15.4(l). Its infrastructure migration is a separately quantified stream and shall not be netted against new-platform effort.

vii. Acceptance-driven. All effort shall be planned to the acceptance gates in section 2.2.5.5 and the milestones in section 2.2.5.6. Deliverables that are not listed against a gate are not deliverables.

2.2.2.15.3 Delivery Model, Phases and Releases

The implementation shall follow the phase structure of section 2.2.5.2, delivered through the WBS in section 2.2.25.6. The phases, their principal outputs and the WBS lines they map to are:

#	Phase	Principal outputs	WBS lines
1	Mobilisation and initiation	Project Initiation Report, Project Management Plan, governance charter and RACI, resource-loaded baseline schedule, RAID register	1.1 – 1.5
2	Requirements validation and business process design	Process catalogue, As-Is maps, To-Be maps, requirements catalogue, fit-gap report, signed requirements baseline	2.1 – 2.6
3	Solution, technical, integration, data and security architecture	Solution Architecture Document, HLD/LLD, integration design, data design, security design, analytics platform design	3.1 – 3.6
4	Build: configuration, development, integration, data migration preparation, environments	Configured modules, workflows, roles and reports; development objects; interfaces and APIs; data quality, mapping and cleansing outputs; DEV/TEST/UAT/PROD/DR environments; RBAC	4.1 – 9.1
5	Test	Test strategy, SIT, regression, performance, security, DR, migration and UAT reports; cutover rehearsals	10.1 – 10.6
6	Change, training and knowledge transfer	Impact assessment, engagement programme, readiness report, TNA, training delivered by audience	11.1 – 12.5
7	Cutover and go-live	Cutover strategy and plan, production migration, go-live, rollback capability	7.7, 13.1 – 13.4
8	Hypercare and transition	Hypercare of 6 months per release, handover pack, as-built pack, lessons learned, closure report, transition to the support and SLA period	14.1 – 15.5

Release strategy. The tenderer shall propose a release strategy and shall state, for each release, the components, sites and user populations included, the cutover approach and the dependency on legacy platforms. KPC's indicative preference, which the tenderer may challenge with justification, is:

Release 1 — ERP and EAM core (finance, budgeting, treasury, supply chain, contracts, projects, asset management) with the electronic procurement service and the legacy ERP infrastructure migration;

Release 2 — MSOOS, TMS and OT integration;

Release 3 — analytics and AI platform, stakeholder management and remaining corporate services.

Where a component is delivered in more than one wave, the build, test, training and cutover effort shall be quantified per wave, and the phase outputs above shall be produced per wave. Phases 1 and 3 are single events for the programme.

2.2.2.15.4 Implementation Scope by Solution Component

For each component below, the scope statement defines what the Contractor implements, the implementation units table gives the countable basis for effort, and the deliverables list identifies what is accepted. Sizing references in brackets refer to section 2.2.6.2.

(a) Enterprise Business Platform — ERP and Enterprise Asset Management

The Contractor shall implement the enterprise business platform covering the Corporate Services, Sales and Commercial Management, Stakeholder Management and Enterprise Asset Management capabilities of sections 2.2.3.1 to 2.2.3.4 and their detailed requirements in section 2.2.4.2, for one legal entity, 26 business units and 3 profit centres, across all sites in reference A2. The scope includes organisation structure and chart of accounts design, configuration of every in-scope functional area, role and authorisation design, workflow configuration, output forms, standard and custom reports, mobile enablement for maintenance and field service on intrinsically safe devices, localisation for Kenyan statutory, tax and regulatory requirements, and the re-implementation of all non-redundant automated processes from the existing landscape.

The Contractor shall implement the Human Capital Management solution proposed under section 2.2.4, together with payroll compliant with all Kenyan statutory requirements (including PAYE, NSSF, SHIF, the Affordable Housing Levy and any other salary component). Workforce planning requirements shall be detailed at blueprinting.

Implementation unit	Basis / source	Quantity
Functional areas (modules) to be configured	Section 2.2.4.2; reference B1	27, comprising Strategic Planning and Performance Management; Governance, Risk and Compliance; Budgeting and Planning; Financial Management; Supply Chain and Inventory; Contract Lifecycle Management; Project Portfolio Management; Order Management; Billing and Revenue Management; Customer Account Management; Pricing Management; Commercial Contracts; Revenue Forecasting; Customer Relationship Management; Supplier Relationship Management; Marketing and Campaign Management; Communications Management; Complaint Management; Maintenance Management; Asset Integrity Management; Work Management; Field Service Management; Maintenance Inventory Management; Reliability and Asset Performance Management; Safety Management; Treasury; Human Capital Management and Payroll
Organisation structure objects	Reference A1	1 legal entity; 26 business units; 3 profit centres; cost centre 570
Named users to be provisioned and role-mapped	Reference A4	1,000 named ERP users; 500 named HR users; Employee Self-Service for 1,500 employees; Manager Self-Service for 150 managers; GRC: 70 approvers and 27 role/ruleset administrators; 500 peak concurrent

Implementation unit	Basis / source	Quantity
Security roles to be designed, built and tested	Section 2.2.6; WBS 4.5 and 9.1	Total roles 3140. However, the roles may overlap, and they are not position based.
Workflows to be configured	Customisation landscape (18 existing); section 2.2.6	Not fewer than 18 existing approval workflows re-implemented;
Reports and dashboards	Reference B12; WBS 4.6 and 5.4	1,000 reports and 100 dashboards in the current landscape to be rationalised.
Migration of Custom Applications within SAP and Other Environments.	Section 2.0.8	The tenderer shall accommodate these functionalities as standard solution or as customization within their proposed solution
Output forms and documents (invoices, purchase orders, delivery notes, statements, certificates, letters)	Section 2.2.4.2	To be provided during Blueprinting
Custom development objects to be rationalised and re-implemented	Customisation landscape: ~85 data extensions, ~120 enhancements, ~200+ programs/reports/forms, ~900 pricing and billing logic objects; WBS 5.1 – 5.3	Report to be rationalised
Master data objects to be structured and loaded	References B3, B5, B6, B7, C2, D1, E10	81,784 maintainable assets; 13,331 stock items; 173,676 fixed asset records; 1,348 projects; 16,000 registered suppliers (2,300 awarded); 232 customers; 1,500 employee records (from e-HR)
Transaction volumes for design, performance testing and cutover planning	References B4, B6	1,688 work orders per month; 556,906 GL journal lines p.a.; 33,977 AP invoices p.a.; 131,859 AR invoices p.a.
Sites for deployment and training	Reference A2	Head Office; 54 pump stations/plants; 7 inland loading terminals; 2 marine discharge terminals; 3 marine loading terminals; 2 aviation terminals; 6 warehouses
Mobile field devices for TMS	Reference N1	40 ATEX-rated inspection tablets under TMS BOM item 4.1
Statutory and regulatory integrations	Section 2.2.3.9	Refer to the scope of integration

Deliverables: configured and documented platform per functional area; configuration workbooks; To-Be process maps and SOPs; role and authorisation matrix with segregation-of-duties ruleset; workflow catalogue; report and form catalogue; development object specifications and code; localisation pack; mobile deployment pack.

(b) Electronic Procurement

The Contractor shall implement the electronic procurement service covering sourcing, supplier registration and lifecycle management, catalogues, requisition-to-order, receipting, invoicing and contract management, integrated to the ERP platform and to the revenue authority e-invoicing system, for KPC's procurement methods under the KPC supply chain policy. The scope includes tenant provisioning, configuration of procurement methods and approval hierarchies, catalogue set-up, supplier onboarding and enablement, the interfaces in reference C10, and training of the requester, approver and procurement power-user populations.

Implementation unit	Basis / source	Quantity
Annual addressable spend under management	Reference C1	KES 17.40 billion
Sourcing methods to be configured, with annual event volumes	Reference C4	Open tender (126 p.a.); restricted (41); request for quotation (146); framework (10); direct (23)
Delegation-of-authority approval levels	Reference C8	Up to 6 levels;
Catalogues	Reference C7	2 (product catalogue, service catalogue);
Supplier population to be migrated and enabled	Reference C2	16,000 registered suppliers migrated; 2,300 awarded suppliers actively enabled; 200 – 300 new registrations p.a.;
Users to be provisioned and trained	Reference C6	800 self-service requesters and approvers; 50 procurement power users
Transaction volumes	References C3, C5	700 requisitions, 500 purchase orders, 2400 invoices p.a. (current); 200 contracts under management; 50 renewals p.a.
Interfaces to the ERP platform	Reference C10; WBS 6.1	Up to 10: supplier master, requisition, goods receipt, invoice, budget check, contract data, chart of accounts and cost centres, material and service master, payment status

Deliverables: provisioned production and non-production tenants; configuration record; DoA and workflow configuration; catalogue load; supplier enablement plan and completion report; interface specifications and test evidence; user and supplier training completion records.

(c) Mid-Stream Oil Operations System (MSOOS)

The Contractor shall implement the MSOOS covering the eleven functional areas of section 2.2.4.2 (Mid-Stream Oil Operations Solution): Planning and Scheduling; Marine Operations; Pipeline Operations and Transportation; Oil Stocks and Inventory Management; Order-to-Cash and Product Delivery Management; Collateral Finance and Financed Inventory Management; Customer Self-Service and Digital Commercial Services; Pricing and Billing Management; Quantity Conversion and Standardisation Management; Master Data Governance and Management; and Planning, Operational Reporting, Audit and Analytics. The scope includes the network, facility and tank model; the central inventory ledger with customer ownership and entitlement; nominations, capacity allocation and scheduling; batch and interface tracking; marine receipt, discharge and backloading; the quantity conversion engine and its standard tables; tariff, pricing and billing rules; the customer and surveyor portals; the revenue authority customs and e-invoicing interfaces; and integration to SCADA, tank gauging, custody transfer metering, laboratory, terminal and ERP systems.

Implementation unit	Basis / source	Quantity
Functional areas and requirement count	Section 2.2.4.2	11 functional areas; requirements as enumerated by identifier (OPS, MO, POT, INV, O2C, CFA, CSS, PB, QC, MDM, PRA)
Pipeline network to be modelled	Reference E1	5 lines: 450 km 20"; 325 km 8"/6"; 325 km 14"; 121 km 6"; 121 km 10"; multi-product;
Stations and transfer points	Reference E2	21 pump stations; 9 delivery points; 4 receipt points
Marine and aviation facilities	Reference A2	2 marine discharge terminals; 3 marine loading terminals; 2 aviation terminals;
Tank and facility model	Reference E9	164 tanks; 1,073,000 m³ total capacity;
Products and quantity conversion tables	Section 2.2.4.2 (Quantity Conversion)	API standards are utilised
Batch operations	Reference E9	18 batches per month (Line 5); 9 batches per month (Lines 4/6)
Customers (shippers) and entitlement accounts	Reference E10	232 customers, of which 160 active; 8 partner-countries
Nominations and order-to-cash volumes	References E10, E11	88,796 nominations per month; 884,283 m³ per month; 1,018 shipper invoices per month
Tariff and pricing structures	Section 2.2.4.2 (Pricing and Billing); customisation landscape (~15 pricing objects)	To be provided during Blueprinting
Collateral finance agreements	Section 2.2.4.2 (CFA)	150 per month
External portals	Section 2.2.4.2 (INV14, MO13, CSS)	Customer self-service portal for 160 active customers; surveyor submission portal;
Sites for deployment and training	References A2, E2	Head Office; 21 pump stations; 7 inland terminals; 5 marine terminals; 2 aviation terminals

Deliverables: functional and detailed design specifications per functional area; network, facility and tank model; configured inventory ledger and entitlement rules; quantity conversion configuration with validation evidence against the declared standards; tariff and billing configuration; portal build; interface specifications; factory acceptance and site acceptance test records; operational procedures and control narratives.

(d) Terminal Management System (TMS) and Terminal Field Equipment

The Contractor shall implement the TMS at each in-scope terminal covering truck and order queue management, truck and driver registration, identification and verification, queue display, safety checklists, loading bay allocation, loading authorisation and automation, and integration to the loading control, metering, gate and MSOOS order-to-cash functions. The scope includes site survey, hazardous-area compliant equipment supply and installation, structured and fibre cabling, industrial network, field devices, per-site configuration, factory and site acceptance testing, and operator, supervisor and transporter training.

Implementation unit	Basis / source	Quantity
Terminals in scope, with loading infrastructure	Reference E8; TMS BOM	5 terminals: PS09 (2 bays, 2 arms, 2 meters, 1 flow computer, 16 loadings/day, 126 hydrant pits); PS25 (6, 12, 12, 5, 714/day); PS27 (12, 22, 22, 8, 912/day); PS28 (10, 27, 27, 15, 706/day); PS10 - commissioning pending
Servers and database platform	TMS BOM items 1.1 – 1.5	10 physical servers; 5 database instances with high availability; 5 administration monitors
Queue display screens	TMS BOM item 2.1	30 outdoor displays
Driver and vehicle processing devices	TMS BOM items 3.2 – 3.4	30 fixed RFID readers (minimum; tenderer to add quantities if required by its design); 150,000 reusable vehicle RFID tags; 10 RFID tag printers/encoders
Inspection devices	TMS BOM item 4.1	40 intrinsically safe inspection tablets
Site network and cabling	TMS BOM items 5.1 – 5.6	2,100 m fibre; 48 dual data points per site (5 sites); 5 industrial 48-port PoE switches; 2 firewall appliances; 30 × 1G and 30 × 10G transceivers
Transporters, trucks and drivers to be registered	TMS BOM item 3.3 (150,000 tags)	To be provided during Blueprinting
Site works	Section 2.2.3.7 (hazardous area compliance)	Civil, cabling, mounting and hazardous-area installation at 5 sites;

Deliverables: site survey reports; per-site design; equipment schedules and hazardous-area compliance certificates; installation completion certificates; factory acceptance test and site acceptance test records per site with punch lists; as-built drawings; operator and transporter training records.

(e) Quality Control Management and Laboratory Integration

The Contractor shall implement quality control management covering product specifications, sampling and test scheduling, results capture, release and quarantine status, certificates of quality, and integration with the existing laboratory information management system and online analysers, so that inventory status and delivery documentation in the MSOOS reflect quality clearance.

Implementation unit	Basis / source	Quantity
Laboratory sites	Reference A2	5
Product specifications and test methods to be configured	Section 2.2.4.2 (Quality Control)	To be provided during Blueprinting
Certificate templates	Section 2.2.4.2 (O2C08)	To be provided during Blueprinting

(f) Cross-Cutting Enterprise Services

The Contractor shall implement the IT Service Management platform, the Enterprise Monitoring and Response platform, the enterprise workflow and business process automation platform, and the integrated

development and low-code platform of section 2.2.4.2, including their processes, integrations to the solution components and to the existing directory and security platforms, and administrator training.

Implementation unit	Basis / source	Quantity
ITSM processes to be configured	Section 2.2.4.2 (TS-ITSM)	Incident, problem, change, release, request, service level, knowledge, CMDB and discovery, asset lifecycle; 41 agents
Monitored estate for the monitoring and response platform	References M2, J7; infrastructure BOM	Infrastructure Architecture to determine the numbers
Development platform users	Reference B2 (3 developer users currently)	10 No.

(g) Enterprise Data Analytics and AI Platform-Assumed cloud deployment

The Contractor shall implement the enterprise data platform comprising data lake and warehouse layers, data integration pipelines from all in-scope sources, data quality and governance tooling, master data management, semantic models feeding the retained visualisation platform, enterprise and regulatory reporting content, and the five priority AI use cases, together with the data engineering and data science tooling for KPC's analytics teams.

Implementation unit	Basis / source	Quantity
Source systems to be integrated	Reference H1	ERP, MSOOS, SCADA, TMS, e-procurement, e-HR and other approved sources;
Analytical data volume	Reference H2	5 TB initial; 10% growth p.a.
Refresh latency	Reference H3	Daily batch standard; near-real-time for approved operational use cases;
Dashboards and reports at go-live	Reference H4; reference B12	Tenderer to propose and validate during design; the current landscape of 100 dashboards and 1,000 reports is the reference baseline;
Analytics users	Reference H5	50, including 10 data engineers/analysts and 5 data scientists
AI and machine learning use cases	Reference H6	5: predictive maintenance; demand forecasting; line performance analytics; operational optimisation; revenue and throughput analytics
Master data domains under governance	Reference I5	Supplier, item, asset, employee, customer, product, tank and facility; Additional details to be provided

Deliverables: data platform design; ingestion pipelines per source; data quality rules and scorecards; master data models and stewardship workflows; semantic models; reporting and dashboard content; five deployed and validated AI use cases with model documentation and monitoring; analytics team enablement records.

(h) Enterprise Integration Platform and Interface Catalogue

The Contractor shall implement the enterprise integration platform comprising API management and developer portal, enterprise service bus and messaging, event streaming, file transfer and integration monitoring, and shall design, build, test, document and support every interface in the interface catalogue across application, IT/OT and external categories.

Implementation unit	Basis / source	Quantity
Interface catalogue baseline	Reference I1	ERP–e-procurement (up to 10 flows); ERP–MSOOS; ERP–e-HR; ERP–revenue authority; ERP–EDRMS; ERP–banks (6 banks, 6 integrations); MSOOS–revenue authority; MSOOS–SCADA; MSOOS–tank gauging; MSOOS–TMS
Existing interfaces to be assessed and re-implemented	Customisation landscape	~45 integration interfaces and flows in the current landscape
Message volumes	Reference I2	6,774 messages per day; peak 6 transactions per second (TPS); annual growth of 11% to be allowed
API consumers	Reference I3	e-procurement, MSOOS, e-HR, revenue authority, EDRMS, banks
Protocols and standards to be supported	Integration landscape; reference E11	REST/JSON; SOAP/XML; SFTP; SWIFT; EDI/XML; OPC UA; event streaming;
Monitoring, alerting and replay	Reference I6	Coverage of all interfaces with alert thresholds, retry and replay rules, reconciliation and retention

(i) Operational Technology Integration

The Contractor shall implement secure integration between the enterprise solution and KPC's operational technology environment in accordance with section 2.2.18, through an IT/OT demilitarised zone with unidirectional or brokered data exchange as required by the security architecture, covering SCADA, tank gauging, custody transfer metering, laboratory, terminal automation, hydrant management, historians, pipeline integrity and operational data repositories. No control system is replaced under this scope.

Implementation unit	Basis / source	Quantity
SCADA systems and historians	Integration landscape	Provided in integration scope
Tank gauging points	Reference E9	164 tanks
Custody transfer and metering points	Reference E8	Not fewer than 29 flow computers across 4 terminals;
Hydrant management	Reference E8	126 hydrant pits at PS09;

(j) Cybersecurity Integration and Access Control

The Contractor shall integrate every solution component with KPC's identity and access management, privileged access management, security information and event management, endpoint security and vulnerability management platforms, shall design and implement centralised role-based access control and segregation of duties across the solution, and shall deliver security testing of the solution before each go-live.

Implementation unit	Basis / source	Quantity
Identities under lifecycle management	Reference M4	2,500 (staff, contractors, suppliers, service accounts)

Implementation unit	Basis / source	Quantity
Single sign-on	Reference D3	Existing identity platform and directory as source of truth; SAML 2.0 and/or OpenID Connect for every component
Privileged accounts	Reference M3	30
SIEM log sources and ingestion	Reference M1	250 GB/day baseline; 5,000 sustained / 10,000 peak EPS; tenderer to declare the log source count per component
Endpoints for endpoint security	Reference M2	2,000
RBAC and segregation-of-duties design	WBS 9.1	To be provided during Blueprinting

(k) Infrastructure Deployment and Environments

The Contractor shall size, supply, install, configure, harden, commission and document the infrastructure of section 2.2.4.2 (Infrastructure Requirements) and the Infrastructure BOM at the Primary Data Centre and the DR site, and shall build and hand over the environment matrix for every solution component. Infrastructure effort shall be quantified separately from application effort.

Implementation unit	Basis / source	Quantity
Hosting sites	References J6, O1, O2	Primary Data Centre at KPC premises (12-rack containerised facility, 200 kW, 144,000 BTU cooling); DR at a managed co-location facility (2 × 42U racks); 79 km separation; 10 Gbps, 2 ms inter-site link
Environments per component	References B10, J7	Production (100%); DR (60%); Training (40%); Quality/UAT (40%); Development (25%) — 5 environments for each hosted component
Compute, virtualisation and container platform	Infrastructure BOM	As specified in the Compute Platform sections for primary and DR sites
Storage	References K1 – K3; Infrastructure BOM	New enterprise storage plus expansion of 2 existing unified storage arrays; tiers 25% flash / 40% SAS / 35% near-line; 10,000 – 64,000+ IOPS; 11% growth p.a.
Backup and recovery	References K4, K5	Weekly full, two-hourly incremental; 7-year retention; disk and tape; immutability
Database platforms and high availability	Infrastructure BOM	As specified, clustered at primary with warm standby at DR
Load balancing, monitoring, automation and orchestration	Infrastructure BOM	As specified

Implementation unit	Basis / source	Quantity
Availability, RPO and RTO	References P1, P2	Tier 1 99.95%; Tier 2 99.90%; Tier 3 99.50%; RPO ≤ 30 min; RTO ≤ 2 h
Capacity headroom	Reference P4	30% above Year-1 volumes at go-live
Disaster recovery testing	Section 2.2.20	Full failover and failback test per release before go-live and annually thereafter

(l) Legacy ERP Infrastructure Migration and Transition

The Contractor shall migrate the existing ERP landscape from its current end-of-life infrastructure to the new infrastructure platform in accordance with section 2.2.3 (Legacy Infrastructure Migration), maintain it in operation until each function is cut over to the new solution, and retain it thereafter in read-only mode for historical access. This stream runs in parallel with, and ahead of, the new-platform build.

Implementation unit	Basis / source	Quantity
Landscape and data volume	Reference B8	20 years of history; 15.5 TB
Environments to be migrated	Section 2.2.3	5: production, quality assurance, development, sandbox, disaster recovery
Interfaces to be re-pointed	Customisation landscape	~45
Database migration	Section 2.2.3	To be confirmed during Blueprinting
Read-only retention period after cutover	Section 2.2.7 (Historical and Archived Data)	8 years
Stabilisation support	Section 2.2.3	Tenderer to declare the stabilisation period assumed

(m) Data Migration

The Contractor shall migrate approved master, open transactional and historical data from the existing ERP and other legacy systems into the new solution components through three mock migrations and a production migration per release, with profiling, cleansing, mapping, transformation, reconciliation, validation and data-owner sign-off for every object, in accordance with section 2.2.7.

Implementation unit	Basis / source	Quantity
Master data objects	References B3, B5, B6, B7, C2, E9, E10	Assets (81,784); stock items (13,331); fixed assets (173,676); projects (1,348); suppliers (16,000); customers (232); tanks (164); contracts (200); other details to be provided during Blueprinting
Open transactional objects	Section 2.2.7	Open AP and AR items; open purchase orders and contracts; open work orders and PM plans; stock balances; GL balances; customer entitlement and inventory ledger

Implementation unit	Basis / source	Quantity
		positions; linefill positions; collateral finance positions;
Historical data to be migrated versus archived	Reference B8; section 2.2.7	To be determined during Inception
Migration cycles	WBS 7.4 – 7.7	3 mock migrations and 1 production migration per release
Data quality and cleansing	WBS 7.1 – 7.3	Tenderer to declare the cleansing effort basis per object, and the split between Contractor cleansing and KPC data-owner cleansing

(n) Testing and Quality Assurance

The Contractor shall plan and execute all test levels in section 2.2.5.2 (Testing Strategy) for every release, provide the test tooling, author test cases and scripts, execute or support execution, manage defects to closure, and produce the test evidence required for each acceptance gate in section 2.2.5.5.

Implementation unit	Basis / source	Quantity
Test levels	Section 2.2.5.2	Unit; configuration and functional; system; system integration; interface; data migration; performance and load; security; disaster recovery and business continuity; regression; user acceptance; operational readiness
Test cycles	WBS 10.2 – 10.6	Not fewer than 2 SIT cycles, 1 regression cycle, 1 performance cycle, 1 UAT cycle and 2 cutover rehearsals per release; tenderer to declare cycles assumed
Test cases	Section 2.2.5.2	Tenderer to declare the number of test cases assumed per component and level, and the tooling proposed
Performance benchmarks	Section 2.2.19 (Technical Performance Benchmarks)	All benchmarks stated, at production-equivalent load with 30% headroom
UAT support	Section 2.2.5.2 (UAT)	Contractor prepares scripts, trains testers, supports execution and manages defects; KPC executes
Defect resolution	Section 2.2.5.2 (Defect Management)	All defects resolved before production deployment;

(o) Organisational Change Management, Training and Knowledge Transfer

The Contractor shall deliver the change management, training and knowledge transfer services of section 2.2.9 for every audience and site, including change impact assessment, stakeholder engagement, business readiness, training needs analysis, training delivery by audience, training materials, knowledge transfer to KPC administrators and support staff, and mentoring through hypercare.

Implementation unit	Basis / source	Quantity
Total workforce in change scope	Reference A3	Approximately 1,500 employees; 11 executives; 38 managers
End users by platform	References A4, C6, H5	ERP and EAM: 1,000; e-procurement: 800 requesters and approvers plus 50 power users; analytics: 50; MSOOS: TMS 200 users to be trained.
External users	References C2, E10; TMS BOM	Suppliers (2,300 awarded); customers (160 active); transporters and drivers 1700. surveyors and financiers 20.
Super users and process owners	Section 2.2.9	70 Superusers and 27 business process owners
Technical and administrator audiences	Section 2.2.9	ICT application, infrastructure, integration, security and analytics administrators; 41
Operational and OT audiences	Section 2.2.9	Control room, terminal and marine operators; 700
Training locations	Reference A2	Head Office and regional sites; OEM sites
Training delivery mode	Section 2.2.9	Instructor-led, train-the-trainer, e-learning;
Training materials	Section 2.2.9	Course materials, quick reference guides, recorded sessions and e-learning modules per audience and per functional area

(p) Cutover, Go-Live, Hypercare and Transition to Support

The Contractor shall plan, rehearse and execute cutover for each release, achieve go-live against the readiness criteria of section 2.2.5.2, provide hypercare, hand over to KPC operations and transition into the support and maintenance services of section 2.2.10.

Implementation unit	Basis / source	Quantity
Cutover events	Section 2.2.5.2; WBS 13	One per release, each with strategy, plan, 2 rehearsals, production migration, go/no-go and rollback capability
Hypercare	WBS 14.1	6 months from each go-live, onsite, with incident resolution to the service levels of section 2.2.10
Warranty	Section 2.2.10 (Warranty)	As stated in section 2.2.10 from each go-live
Handover and closure	WBS 15.1 – 15.4	Handover pack, as-built pack, lessons learned, closure report
Support and maintenance	WBS 15.5; section 2.2.10	36-month service level agreement following Final Acceptance,

Implementation unit	Basis / source	Quantity
		covering application, infrastructure, integration and security support
Support transition	Section 2.2.10 (Support Transition)	Transition plan and knowledge retention from hypercare into the SLA period

(q) Programme Management, Governance and Reporting Obligations

The Contractor shall provide its own project management for Lot 2, operating within the programme governance framework administered by the Lot 1 Programme Management Office, and shall include in its effort the governance, reporting, stage-gate and quality obligations of sections 2.2.21 and 2.2.24.

Implementation unit	Basis / source	Quantity
Governance forums	Section 2.1 (Programme Governance Structure); section 2.2.5.15	Steering committee, programme board, design authority, change control board, working groups; PMO Vendor to propose
Reporting	Section 2.1 (Reporting Requirements); section 2.2.5.15	Weekly progress, monthly programme, stage-gate and exception reports
Stage gates	Section 2.1 (Stage Gate Reviews); section 2.2.5.6	One per milestone in section 2.2.5.6
Key personnel and onsite presence	Section 2.2.24 (Resource Requirements)	Tenderer to declare the key personnel, their onsite percentage per phase and the FTE profile per phase

2.2.2.15.5 Effort Estimation Matrix

The tenderer shall quantify every WBS line in the Implementation Services BOM using the unit of measure and quantity basis below. Where the quantity is drawn from this section or section 2.2.6.2 it is fixed for the purposes of the tender; where it is to be declared, the tenderer's declared value becomes the contractual basis of estimate on award.

WBS	Activity	Unit	Quantity basis
1	Project initiation	Lot / document	1 programme; one PIR, PMP, governance charter, baseline schedule and RAID register
2.1 – 2.3	Process discovery, As-Is and To-Be design	Process	Process count per functional area, to be determined during blueprinting across ERP/EAM (27 areas), MSOOS (11 areas), e-procurement and TMS
2.4	Requirements validation	Requirement	All requirements enumerated by identifier in sections 2.2.4.2 and 2.2.6
2.5	Fit-gap analysis	Module / process	27 ERP/EAM areas; 11 MSOOS areas; e-procurement; TMS; cross-cutting services; analytics
2.6	Requirements baseline	Lot	1 per release
3.1 – 3.6	Architecture	Lot	1 programme set, updated per release
4.1	ERP module configuration	Module	27 functional areas

WBS	Activity	Unit	Quantity basis
4.2	MSOOS configuration	Functional area / site	11 functional areas; 5 lines; 21 stations; 164 tanks; 7 inland, 5 marine and 2 aviation terminals
4.3	TMS configuration	Terminal	5 terminals;
4.4	Workflow configuration	Workflow	Not fewer than 18;
4.5	Role configuration	Role	To be declared by tenderer against KPC's current role count
4.6	Reporting configuration	Report	To be declared by tenderer against the 1,000-report, 100-dashboard baseline
5.1 – 5.3	Development objects	Object	To be declared by tenderer, by complexity, after rationalisation of ~85 extensions, ~120 enhancements, ~200+ programs and ~15 pricing objects
5.4	Custom reports	Report	To be declared by tenderer
6.4	API development	API	To be declared by tenderer
7.1 – 7.3	Data profiling, mapping, cleansing	Data object	Master and open transactional objects listed in 2.2.2.15.4(m); full list to be determined at blueprinting
7.4 – 7.7	Mock and production migrations	Cycle	3 mock and 1 production per release
8.1 – 8.5	Environments	Environment	5 per hosted component (DEV, TEST/QA, TRN, PROD, DR) at the ratios in reference J7
9.1	RBAC design and implementation	Lot	1 programme; 2,500 identities;
10.1 – 10.6	Testing	Cycle	Per release: ≥2 SIT, 1 regression, 1 performance, 1 UAT, 2 cutover rehearsals; security and DR tests per release
11.1 – 11.3	Change management	Lot	1 programme; ~1,500 staff; all sites in reference A2
12.1 – 12.5	Training	Session	Audiences and counts in 2.2.2.15.4(o); tenderer to declare sessions per audience per site
13.1 – 13.4	Cutover and deployment	Release	Number of releases per tenderer's release strategy
14.1 – 14.2	Hypercare	Month	6 months per release
15.1 – 15.4	Handover and closure	Lot	1 programme
15.5	Support and maintenance	Month	24 months

2.2.2.15.6 KPC-Provided Resources and Dependencies

The tenderer shall base its estimate on the following being provided by KPC. Where the tenderer requires more than is stated, the additional requirement shall be declared under section 2.2.2.15.8.

i. Process owners and subject matter experts for each functional area, available for workshops, design sign-off and UAT .

ii. Super users nominated per functional area and per site, released for training and UAT.

iii. Data owners per master data domain, responsible for cleansing decisions and migration sign-off.

iv. Access to existing systems, documentation, configuration, custom object inventories, interface specifications and the current process catalogue.

v. Data centre space, power, cooling, network connectivity and physical access at the Primary Data Centre and the DR site as described in references O1, O2 and L4.

vi. Site access, permits to work and safety inductions at operational sites.

vii. Programme Management Office services under Lot 1, including programme governance, integrated reporting and stage-gate administration.

viii. Licences and administration of the retained platforms (visualisation, directory, security platforms, SCADA and control systems). The bidder may provide alternative visualization tools.

ix. Test environments for external counterparties (revenue authority, banks) and the coordination of those counterparties.

2.2.2.15.7 Exclusions and Scope Boundaries

The following are outside the implementation scope of Lot 2. Integration with them, where listed in section 2.2.2.15.4, is within scope.

i. The Electronic Document and Records Management System, which is procured separately; the ERP–EDRMS interface is within scope.

ii. Wide-area and local-area network refresh at operational sites (reference L3), other than the terminal networks in the TMS BOM.

iii. End-user computing devices other than the intrinsically safe tablets and terminal devices listed in the BOM.

iv. Civil works at operational sites other than those required for TMS field equipment installation.

2.2.2.15.8 Assumptions the Tenderer Shall Declare

The tenderer shall submit, with its Implementation Services BOM, a Basis of Estimate statement covering each item below. Absence of a declaration means the tenderer has assumed the most onerous reading of the requirement.

#	Item	Declaration required
1	Release strategy	Number of releases; components, sites and users per release; dependencies on legacy platforms
2	Resource profile	Full Time Equivalent (FTE) by role by phase; onsite/offsite split; named key personnel and their onsite percentage
3	Declared quantities	Every quantity marked in this section for tenderer declaration, with the basis for each
4	Rationalisation basis	Method and outcome of rationalising the existing customisation landscape into simple, medium and complex development objects
5	KPC resource assumptions	Availability of process owners, SMEs, super users and data owners assumed, where different from section 2.2.2.15.6
6	Working pattern	Working days, hours, public holidays, travel and subsistence basis, and whether site work is priced at the site
7	Tooling	Test management, migration, integration, monitoring and documentation tooling proposed and whether licences are included
8	Subcontracting and OEM effort	Which scope is delivered by OEMs, consortium members or subcontractors, and how their effort is included

#	Item	Declaration required
9	Contingency	Contingency included in the effort and the risks it covers
10	Exclusions	Any scope the tenderer has excluded, with reasons; an exclusion not declared here is deemed included

2.2.4 Specifications

2.2.4.1 *Solution Architecture and Design Requirements*

The Tenderer shall propose and implement a comprehensive Solution Architecture that provides an integrated, secure, scalable and resilient technology environment for all components of the Enterprise Digital Transformation Solution.

The proposed architecture shall align the enterprise applications, operational systems, data platforms, integration services, cybersecurity capabilities, ICT infrastructure and Operational Technology (OT) environment into a coherent and sustainable architecture.

2.2.4.1.1 Enterprise Architecture

During the implementation period the Contractor shall develop a detailed Enterprise Solution Architecture covering the business, application, data, integration, technology, security and infrastructure layers.

The architecture shall:

a) support the approved requirements and To-Be business processes;

b) provide clear separation of business applications, shared services, integration services, data platforms, infrastructure and security services;

c) support modularity and interoperability between solution components;

d) minimise unnecessary customisation and favour standard, configurable and upgradeable product capabilities;

e) support scalability and future expansion without major architectural redesign;

f) provide high availability and resilience for critical business and operational workloads;

g) support integration with KPC's existing and future systems; and

h) provide comprehensive technical and architectural documentation for all implemented components.

2.2.4.1.2 Application Architecture

The application architecture shall provide an integrated environment for the ERP, MSOOS, TMS, Enterprise Data Analytic and AI Platform, Integration Platform and other enterprise applications.

The architecture shall support appropriate separation of Development, Test, User Acceptance Testing and Production environments.

The Contractor shall ensure that application components are appropriately configured, integrated and secured and that dependencies between applications are clearly identified and documented.

2.2.4.1.3 Data Architecture

The Contractor shall develop a comprehensive data architecture covering transactional data, master data, operational data, analytical data, historical data and reporting requirements.

The architecture shall support:

a) Operational Data Stores;

b) enterprise data lake capabilities;

c) Master Data Management;

d) data integration and synchronisation;

e) data cleansing and transformation;

f) data quality and validation;

g) data lineage and traceability;

h) enterprise reporting and analytics;
i) controlled access to data; and
j) data governance and retention requirements.

2.2.4.1.4 Integration Architecture

The Contractor shall develop an integration architecture providing secure and reliable interoperability between KPC's enterprise applications, operational systems, OT environment and approved external systems.

The architecture shall support, as applicable:
a) REST, SOAP, OData or equivalent standards-based APIs;
b) API Management and API Developer Portal capabilities;
c) Enterprise Service Bus and middleware;
d) event-driven integration and event streaming;
e) workflow integration;
f) data synchronisation;
g) secure file and message-based integration;
h) Service Mesh capabilities where applicable; and
i) monitoring, logging and management of integrations.

The Contractor shall ensure that integration services are designed for reliability, scalability, security, maintainability and future reuse.

2.2.4.1.5 Infrastructure Architecture

The Contractor shall develop the infrastructure architecture supporting the Primary Data Centre and Disaster Recovery environment.

The architecture shall cover compute, storage, databases, virtualization, containerization, networking, load balancing, operating systems, backup, monitoring, high availability and other supporting infrastructure.

The infrastructure shall be appropriately sized based on the proposed solution architecture, expected workloads, user volumes, transaction volumes, data growth, performance requirements and future expansion.

2.2.4.1.6 Disaster Recovery and Business Continuity Architecture

The Contractor shall design and implement an appropriate Disaster Recovery and Business Continuity architecture for critical workloads.

The architecture shall support a **Recovery Point Objective (RPO) of not more than thirty (30) minutes and a Recovery Time Objective (RTO) of not more than two (2) hours** for critical workloads.

The Contractor shall provide the necessary replication, backup, recovery, failover, monitoring and testing capabilities to achieve the required recovery objectives.

2.2.4.1.7 Security Architecture

The Contractor shall develop a security architecture aligned with KPC's existing cybersecurity environment and applicable security standards.

The architecture shall support integration with KPC's IAM, PAM and SIEM platforms and shall provide appropriate controls for authentication, authorisation, privileged access, encryption, audit logging, vulnerability management, security monitoring and security incident management.

The Solution shall support Single Sign-On (SSO), Multi-Factor Authentication (MFA), SAML 2.0, OAuth 2.0, OpenID Connect, SCIM and LDAP, as applicable to the proposed solution and KPC's identity architecture.

2.2.4.1.8 IT/OT Architecture

The Contractor shall develop an architecture that provides secure integration between the enterprise IT environment and KPC's OT environment.

The architecture shall maintain appropriate network segregation, access controls, monitoring, security controls and integration boundaries between IT and OT environments.
The Contractor shall ensure that integration with SCADA, Terminal Automation Systems, ATG, LIMS, PIMS, OT historians and other OT platforms does not compromise the availability, integrity or security of operational systems.

2.2.4.1.9 Cloud and Deployment Architecture

The Contractor shall clearly define the proposed deployment model for each solution component, including On-Premises, Private Cloud, Public Cloud, Hybrid Cloud or other approved deployment models.
Where cloud services are proposed, the Contractor shall clearly identify the cloud provider, hosting location, data residency arrangements, disaster recovery location, service dependencies, security controls and applicable licensing or subscription arrangements.
The proposed architecture shall comply with KPC's data sovereignty, security and regulatory requirements.

2.2.4.1.10 Architecture Standards and Technology Lifecycle

All proposed technology components shall be current, commercially supported and within the OEM's active product lifecycle at the time of implementation.
The Contractor shall not introduce End-of-Life (EOL), End-of-Support (EOS) or otherwise unsupported components into the Solution.
The Contractor shall provide product roadmaps, support lifecycle information and upgrade policies for all major solution components and shall ensure that the proposed architecture remains supportable throughout the Contract and applicable support period.

2.2.4.1.11 Architecture Deliverables

The Contractor shall submit detailed architecture documentation for KPC's review and approval before implementation of the corresponding solution components.
The architecture documentation shall include, as applicable, enterprise architecture, application architecture, data architecture, integration architecture, infrastructure architecture, security architecture, IT/OT architecture, disaster recovery architecture, deployment architecture and detailed technical designs.
No material implementation shall commence until the relevant architecture, and design documents have been reviewed and approved by KPC.

2.2.4.2 *Detailed Functional requirements*

2.2.4.2.1 Corporate Services

2.2.4.2.1.1 Strategic Planning and Performance Management

Overview

The proposed solution should provide an integrated Strategic Planning and Performance Management capability that enables the Corporation to formulate, align, execute, monitor, evaluate, and continuously improve its corporate strategy, business plans, programmes, projects, strategic initiatives, and organizational performance.

The solution should support strategic environmental analysis, strategic objective setting, cascading of objectives and targets, performance measurement, programme and portfolio monitoring, forecasting, monitoring and evaluation, executive decision-making, and regulatory reporting through configurable workflows, dashboards, analytics, and enterprise-wide collaboration.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
SPM01	Corporate Strategy Management	The system should support strategic environmental scanning, SWOT/PESTLE analysis, formulation, review, approval, publication, execution, and monitoring of Corporate Strategic Plans, business plans, departmental plans, and operational plans. It should support definition of strategic themes, priorities, objectives, assumptions, dependencies, and alignment of departmental and operational plans to corporate strategy, with version control and periodic strategy reviews.		
SPM02	Performance Planning and Target Management	The system should support definition, cascading, alignment, approval, monitoring, and evaluation of strategic objectives, KPIs, performance contracts, scorecards, targets, and performance initiatives across all organizational levels.		
SPM03	Strategic Initiatives, Programme and Portfolio Performance Management.	The system should support planning, prioritization, execution monitoring, evaluation, benefits realization, resource monitoring, risk and dependency tracking, and reporting of strategic initiatives, programmes, projects, and portfolios in alignment with corporate objectives.		
SPM04	Corporate Planning and Forecasting	The system should support corporate planning, demand forecasting, scenario modelling, what-if analysis, economic analysis, tariff planning, resource planning,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		and strategic forecasting to support informed management decision-making.		
SPM05	Monitoring, Evaluation and Performance Reporting	The solution shall support monitoring, evaluation, milestone tracking, variance analysis, organizational performance measurement, and reporting through configurable dashboards and scorecards.		
SPM06	Data Collection and Performance Analytics	The solution shall support collection, validation, consolidation, analysis, visualization, and reporting of strategic and operational performance data from multiple internal and external sources.		
SPM07	Workflow and Collaboration	The solution shall support configurable workflows for planning, approvals, stakeholder reviews, document collaboration, notifications, reminders, and escalations throughout the planning lifecycle.		
SPM08	Continuous Improvement and Knowledge Management	The solution shall support lessons learned, corrective actions, improvement initiatives, benchmarking, maturity assessments, innovation tracking, and organizational learning.		
SPM09	Executive Reporting and Dashboards	The solution shall provide executive dashboards, balanced scorecards, KPI dashboards, predictive analytics, trend analysis, statutory reports, board reports, and self-service reporting capabilities.		
SPM10	Integration and Governance	The solution shall integrate with Budgeting & Planning, Financial Management, Project Portfolio Management, Human Capital Management, Governance, Risk & Compliance, Enterprise Asset Management, and other enterprise applications while providing role-based security, audit trails, and version control.		

2.2.4.2.1.2 Governance, Risk and Compliance (GRC)

Overview

The proposed solution shall provide an integrated Governance, Risk & Compliance (GRC) capability to enable the Corporation to establish effective governance structures, identify and manage enterprise risks, ensure compliance with statutory and regulatory obligations, strengthen

internal controls, support internal and external audits, manage policies and delegated authorities, and provide executive visibility into the organization's governance and compliance posture.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
GRC01	Enterprise Risk Management	The solution shall support identification, assessment, analysis, evaluation, treatment, monitoring, and reporting of strategic, operational, financial, ICT, project, health, safety, environmental, and compliance risks using configurable risk methodologies.		
GRC02	Internal Controls Management	The solution shall support design, implementation, documentation, monitoring, testing, and continuous evaluation of internal controls, including preventive, detective, and corrective controls across business processes.		
GRC03	Governance Reporting and Analytics	The solution shall provide configurable dashboards, risk heat maps, compliance scorecards, audit dashboards, executive reports, trend analysis, key risk indicators (KRIs), KPI reporting, and self-service analytics with drill-down capabilities.		

2.2.4.2.1.3 Budgeting and Planning

Overview

The proposed solution shall provide an integrated Budgeting & Planning capability that enables the Corporation to prepare, review, approve, execute, monitor, and control strategic, operational, and capital budgets. The solution shall support collaborative planning, forecasting, scenario analysis, budget execution, funds control, and performance monitoring while ensuring alignment between corporate strategy, programmes, projects, and financial resources.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
BP01	Strategic Budget Planning	The solution shall support preparation of strategic, operational, capital, departmental, programme, and project budgets aligned with the Corporation's strategic objectives, business plans, and annual work plans.		
BP02	Budget Preparation and Consolidation	The solution shall support decentralized, Hierarchical, budget preparation, authoring, collaborative planning, budget submissions, consolidation, reviews, approvals, revisions, and		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		version management across all organizational units. Approved budgets should be posted to respective GLs , Cost Centres and projects for utilizations.		
BP03	Budget Allocation and Funds Management	The solution shall support allocation of budgets across business units, cost centres, departments, projects, funds, and programmes while enforcing configurable funding rules and budget controls.		
BP04	Budget Execution and Control	The solution shall support budget commitments, funds availability checks, budget reservations, transfers, reallocations, supplementary budgets, expenditure monitoring, and budget utilization tracking.		
BP05	Forecasting and Scenario Planning	The solution shall support rolling forecasts, demand forecasting, cash flow forecasting, revenue and expenditure forecasting, scenario modelling, what-if analysis, and predictive planning.		
BP06	Programme and Project Financial Planning	The solution shall support planning, budgeting, monitoring, and reporting of capital projects, operational projects, grants, donor-funded initiatives, and other strategic programmes throughout their lifecycle.		
BP07	Budget Performance Monitoring	The solution shall support monitoring of budget utilization, variance analysis, expenditure trends, financial performance, KPIs, and achievement of planned outcomes through configurable dashboards and alerts.		
BP08	Workflow and Budget Governance	The solution shall support configurable workflows for budget preparation, approvals, revisions, submissions, delegations, notifications, audit trails, document attachments, and complete traceability of budgeting activities.		
BP09	Budget Reporting and Analytics	The solution shall provide real-time budget reports, budget versus actual analysis, variance reporting, executive dashboards, forecasting reports, utilization dashboards, drill-down analytics, and self-service reporting capabilities.		
BP10	Integration and Governance	The solution shall integrate seamlessly with Strategic Planning & Performance Management, Financial Management, Supply Chain & Electronic Procurement, Contract Lifecycle Management, Human Capital & Payroll, Project		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Portfolio Management, Enterprise Asset Management, and other enterprise applications while maintaining a single source of financial planning information, role-based security, and comprehensive auditability.		

2.2.4.2.1.4 Financial Management

Overview

The proposed solution should provide a comprehensive Financial Management capability that enables the Corporation to manage financial accounting, budgeting, accounts payable, accounts receivable, treasury, taxation, fixed assets, project accounting, financial controls, consolidation, financial reporting, and financial governance.

The solution should support real-time financial processing, budgetary and financial controls, secure electronic payments, statutory compliance, auditability, and integration with enterprise business functions to provide a controlled and auditable source of financial information.

The solution should support accounting recognition, measurement, presentation, disclosure, and reporting in accordance with applicable IFRS, IAS, GAAP principles, Kenyan statutory and regulatory requirements, tax legislation, and the Corporation's approved accounting policies. Where applicable, the solution should support other prescribed accounting frameworks and reporting requirements.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
FM01	**General Ledger and Financial Accounting**	The solution should support General Ledger, Chart of Accounts, multi-company, multi-currency, multi-fund accounting, journal processing, recurring journals, accruals, provisions, prepayments, reversals, allocations, intercompany transactions, financial period management, account reconciliation, Cost Centre accounting, Profit Centre accounting, Funds Centre accounting, Internal Orders, activity-based costing, overhead allocations, profitability analysis, financial dimensions, and automated accounting processes.		
FM02	**Accounts Payable, Travel**	The solution shall support supplier invoice processing, invoice matching,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	and Expense Management	payment requests, employee claims, travel requests, imprests, advances, expense reimbursements, per diem calculations, retention management, payment approvals, supplier reconciliation, policy compliance, expense auditing, and electronic payment processing.		
FM03	**Accounts Receivable, Debtors and Revenue Management**	The solution should support accounts receivable and debtor management by receiving customer invoice data from the billing system and processing receipts, payment allocation, reconciliation, credit management, collections, dunning, disputes, payment arrangements, debtor ageing, overdue debt management, write-offs, recoveries, revenue recognition, and receivables reporting.		
FM04	**Treasury, Banking and Cash Management**	The solution shall support bank account management, cash positioning, liquidity management, payment scheduling, electronic funds transfers, payment runs, bank integrations, SWIFT messaging, Host-to-Host (H2H) connectivity, investments, borrowing and lending management, foreign exchange management, bank statement processing, bank reconciliation, actual and forecast cash flow, treasury risk management, and cheque management.		
FM05	**Fixed Assets and Lease Accounting**	The solution shall support acquisition, capitalization, depreciation, revaluation, transfers, impairment, insurance, maintenance costing, retirement, disposal, lease lifecycle management, right-of-use assets, lease liabilities, lease modifications, lease payments, and financial accounting for assets throughout their lifecycle in compliance with applicable accounting standards.		
FM06	**Taxation and Statutory Compliance**	The solution shall support management of VAT, Withholding Tax, Withholding VAT, statutory levies, corporate taxes, regulatory reporting, electronic tax submissions, tax codes, and		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		compliance with applicable statutory, regulatory, and financial reporting requirements.		
FM07	**Project Accounting, Financial Close and Consolidation**	The solution should support project accounting, project cost tracking, WBS-based accounting, project expenditure and revenue tracking, project settlement, period-end and year-end closing, financial reconciliations, foreign currency revaluation, provisions, financial adjustments, financial consolidation, intercompany eliminations, and preparation of consolidated financial statements		
FM08	**Financial Controls and Governance**	The solution shall support configurable approval workflows, segregation of duties, delegated authorities, audit trails, financial controls, exception management, document attachments, compliance monitoring, workflow automation, and complete transaction traceability.		
FM09	**Financial Reporting and Analytics**	The solution shall provide configurable financial statements, management reports, statutory reports, executive dashboards, profitability analysis, cash flow reports, budget versus actual analysis, financial KPIs, performance scorecards, predictive analytics, drill-down analytics, and self-service reporting capabilities.		
FM10	**Shared Financial Services**	The solution shall support centralized financial shared services including shared accounts payable, shared accounts receivable, centralized treasury operations, centralized financial processing, workload management, service level monitoring, workflow automation, exception handling, and standardized financial service delivery across multiple business units.		
FM11	**Integration and Electronic Payments**	The solution shall support seamless integration with Budgeting & Planning, Supply Chain & Electronic Procurement, Contract Lifecycle Management, Human Capital &		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Payroll, Project Portfolio Management, Enterprise Asset Management, Customer Management, Business Intelligence, banking platforms, taxation systems, payment gateways, and other enterprise applications while maintaining financial integrity, secure electronic payments, role-based security, and comprehensive auditability.		
FM12	**Financial Master Data and Governance**	The solution shall support centralized management and governance of financial master data including chart of accounts, company codes, fiscal calendars, currencies, exchange rates, tax codes, payment terms, business partners, bank master data, financial dimensions, validation rules, version control, data quality, and complete master data governance.		

2.2.4.2.1.5 Supply Chain and Electronic Procurement

Overview

The proposed solution shall provide an integrated Supply Chain & Electronic Procurement capability that supports the complete procurement lifecycle from demand planning to supplier payment. The solution shall enable efficient sourcing, procurement planning, inventory replenishment, contract execution, supplier collaboration, warehouse operations, logistics management, and statutory procurement compliance while promoting transparency, accountability, and operational efficiency.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
SCM01	Procurement Planning and Demand Management	The solution shall support annual procurement planning, demand forecasting, procurement requisitions, procurement scheduling, procurement budgeting, consolidation of requirements, and monitoring of procurement plans.		
SCM02	Requisition and Approval Management	The solution shall support creation, review, approval, amendment, cancellation, tracking, and electronic routing of purchase requisitions using configurable workflows and delegated authority matrices.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
SCM03	Strategic Sourcing and Tender Management	The solution shall support RFIs, EOIs, RFQs, RFPs, tenders, reverse auctions, bid receipt, bid evaluation, supplier communications, tender awards, and electronic procurement processes in compliance with applicable procurement regulations.		
SCM04	Purchase Order Management	The solution shall support purchase order creation, approvals, amendments, release, dispatch, acknowledgement, tracking, receipt confirmation, and closure with full auditability.		
SCM05	Supplier Management	The solution shall support online supplier registration, onboarding, qualification, categorization, performance evaluation, compliance monitoring, supplier collaboration, supplier self-service, and centralized maintenance of supplier master data.		
SCM06	Inventory and Warehouse Management	The solution shall support inventory planning, stock control, warehouse operations, goods receipt, goods issue, stock transfers, stock counting, valuation, replenishment, reservations, batch and serial number management, and inventory optimization.		
SCM07	Logistics and Materials Management	The solution shall support materials planning, transportation coordination, delivery scheduling, warehouse logistics, material movements, inventory visibility, and tracking of materials throughout the supply chain.		
SCM08	Procurement Compliance and Governance	The solution shall support procurement governance, delegated authority, approval workflows, segregation of duties, procurement audit trails, regulatory compliance, document management, exception management, and complete traceability of procurement activities.		
SCM09	Procurement Reporting and Analytics	The solution shall provide procurement dashboards, spend analysis, supplier performance reports, inventory reports, procurement KPI monitoring, savings analysis, compliance reporting, executive dashboards, and self-service reporting with drill-down capabilities.		
SCM10	Integration and Governance	The solution shall integrate seamlessly with Budgeting & Planning, Financial Management, Contract Lifecycle Management, Supplier		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Relationship Management, Enterprise Asset Management, Enterprise Document Management, Digital Signature Platform, and other enterprise applications while providing role-based security, workflow automation, notifications, audit trails, and end-to-end visibility across the supply chain lifecycle.		

2.2.4.2.1.6 Contract Lifecycle Management

Overview

The proposed solution shall provide an integrated Contract Lifecycle Management (CLM) capability to manage the complete contract lifecycle from contract request and authoring through negotiation, review, approval, execution, performance monitoring, amendments, renewals, obligations management, and contract close-out. The solution shall enhance governance, compliance, transparency, supplier collaboration, and contract performance while integrating seamlessly with procurement, finance, project management, and document management functions.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CLM01	Contract Request and Initiation	The solution shall support contract requests, business justification, contract planning, approval workflows, contract categorization, risk assessment, and initiation of contract lifecycle activities.		
CLM02	Contract Authoring and Document Management	The solution shall support configurable contract templates, clause libraries, document generation, collaborative authoring, document version control, redlining, and centralized contract document management.		
CLM03	Contract Review, Negotiation and Approval	The solution shall support collaborative contract reviews, legal review, negotiations, comments, approval workflows, delegated authority, stakeholder collaboration, and complete audit trails throughout the approval process.		
CLM04	Contract Execution and Digital Signing	The solution shall support electronic contract execution, digital signatures, execution workflows, witness management, execution status tracking, and secure storage of executed agreements.		
CLM05	Contract Performance and	The solution shall support monitoring of contractual obligations, deliverables,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Obligation Management	milestones, service levels, key performance indicators (KPIs), payment milestones, compliance requirements, and contract performance throughout the contract period.		
CLM06	Contract Change, Renewal and Closure Management	The solution shall support contract amendments, change orders, extensions, renewals, variations, terminations, expiry management, contract close-out, and archival in accordance with organizational policies.		
CLM07	Supplier and Stakeholder Collaboration	The solution shall support secure collaboration with suppliers, contractors, consultants, legal teams, project teams, and other stakeholders throughout the contract lifecycle, including correspondence and document exchange.		
CLM08	Contract Governance and Compliance	The solution shall support compliance monitoring, contractual risk management, delegated authority, workflow automation, audit trails, exception management, alerts, reminders, and regulatory compliance throughout the contract lifecycle.		
CLM09	Contract Reporting and Analytics	The solution shall provide configurable dashboards, contract registers, obligation tracking reports, expiry reports, supplier performance reports, spend analysis, compliance reports, executive dashboards, and self-service reporting with drill-down capabilities.		
CLM10	Integration and Governance	The solution shall integrate seamlessly with Supply Chain & Electronic Procurement, Financial Management, Project Portfolio Management, Enterprise Document & Records Management, Digital Signature Platform, Supplier Relationship Management, Enterprise Asset Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and complete traceability of all contract lifecycle activities.		

2.2.4.2.1.7 Human Capital and Payroll Management

Overview

The proposed solution shall provide an integrated Human Capital & Payroll Management capability that supports the complete employee lifecycle from workforce planning, recruitment, onboarding, and employee administration through performance management, learning and

development, payroll processing, employee engagement, succession planning, and separation. The solution shall enhance workforce productivity, ensure statutory compliance, streamline HR operations, and provide employees and managers with secure self-service capabilities.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
HCM01	Workforce Planning and Establishment Management	The solution shall support workforce planning, organizational structure management, establishment control, position management, manpower planning, succession planning, and workforce analytics aligned with the Corporation's strategic objectives.		
HCM02	Recruitment and Onboarding	The solution shall support manpower requisitions, recruitment planning, vacancy management, applicant tracking, interview management, candidate evaluation, onboarding, probation management, employee induction, and Staff Cards Management.		
HCM03	Employee Administration	The solution shall support employee master data management, employment lifecycle management, appointments, transfers, promotions, confirmations, disciplinary processes, employee movements, separation, retirement, and maintenance of complete employee records.		
HCM04	Time, Attendance and Leave Management	The solution shall support work schedules, attendance management, overtime, shift management, leave planning, leave approvals, absence management, timesheets, and integration with biometric and attendance systems where applicable.		
HCM05	Payroll and Benefits Management	The solution shall support payroll processing, earnings and deductions, statutory contributions, pensions, loans, advances, benefits administration, gratuity, final dues processing, payroll reconciliation, Staff Medical Scheme and Clinic Management, and statutory reporting. The payroll system should be configurable to ensure continuous compliance to changing legal and regulatory environment with Kenya.		
HCM06	Performance, Learning and	The solution shall support performance planning, performance appraisals, competency management, training needs		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Talent Management	analysis, learning management, certifications, career development, succession planning, and talent management.		
HCM07	Employee and Manager Self-Service	The solution shall provide secure self-service capabilities for employees and managers, including personal information updates, leave applications, approvals, payslips, performance reviews, training requests, workflow approvals, and organizational communications.		
HCM08	HR Governance and Compliance	The solution shall support HR policies, delegated authority, approval workflows, document management, employee disciplinary processes, grievance management, occupational health and safety records, audit trails, and compliance with applicable labour laws and organizational policies.		
HCM09	HR Reporting and Workforce Analytics	The solution shall provide configurable dashboards, workforce analytics, payroll reports, establishment reports, leave reports, diversity reports, statutory reports, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
HCM10	Integration and Governance	The solution shall integrate seamlessly with Financial Management, Budgeting & Planning, Project Portfolio Management, Enterprise Document & Records Management, Digital Signature Platform, IT Service Management, Identity & Access Management, and other enterprise applications while providing role-based security, workflow automation, notifications, audit trails, and complete traceability of all human capital and payroll activities.		

2.2.4.2.1.8 Project Portfolio Management

Overview

The proposed solution shall provide an integrated Project Portfolio Management (PPM) capability that supports the planning, prioritization, execution, monitoring, governance, and delivery of capital and operational projects throughout their lifecycle. The solution shall enable effective portfolio governance, resource optimization, schedule and cost control, risk management, contract administration, benefits realization, and performance reporting while integrating seamlessly with finance, procurement, asset management, and strategic planning.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
PPM01	Project Portfolio Planning and Prioritization	The solution shall support project proposal management, portfolio planning, business case management, project evaluation, prioritization, investment planning, portfolio optimization, approvals, and alignment of projects with the Corporation's strategic objectives.		
PPM02	Project Planning and Scheduling	The solution shall support project planning, Work Breakdown Structures (WBS), scheduling, milestones, dependencies, baseline management, resource planning, critical path analysis, and project lifecycle management.		
PPM03	Project Cost and Budget Management	The solution shall support project budgeting, cost estimation, cost allocation, commitments, expenditure tracking, forecasts, earned value management, financial controls, and budget versus actual analysis throughout the project lifecycle.		
PPM04	Resource and Capacity Management	The solution shall support planning, allocation, utilization, scheduling, and optimization of human resources, contractors, equipment, materials, and other project resources across multiple projects and portfolios.		
PPM05	Project Execution and Delivery Management	The solution shall support execution, progress tracking, milestone management, deliverables management, issue management, change control, project collaboration, and project documentation throughout the implementation lifecycle.		
PPM06	Project Risk, Quality and Governance	The solution shall support project risk management, issue management, quality assurance, governance reviews, stage gate approvals, compliance monitoring, audit trails, lessons learned, and corrective action management.		
PPM07	Project Contract and Procurement Integration	The solution shall support management of project-related procurement, contracts, supplier deliverables, payment milestones, variation orders, contract performance, and integration with procurement and contract lifecycle management processes.		
PPM08	Project Monitoring,	The solution shall support real-time monitoring of project performance, KPIs, schedules, costs, resource utilization, benefits realization,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Reporting and Benefits Realization	executive dashboards, portfolio reporting, trend analysis, and self-service reporting with drill-down capabilities.		
PPM09	Project Document and Collaboration Management	The solution shall support centralized project document management, version control, collaboration, workflow automation, approvals, correspondence management, meeting management, and integration with the Enterprise Document & Records Management solution.		
PPM10	Integration and Governance	The solution shall integrate seamlessly with Strategic Planning & Performance Management, Budgeting & Planning, Financial Management, Supply Chain & Electronic Procurement, Contract Lifecycle Management, Enterprise Asset Management, Human Capital & Payroll Management, Enterprise Document & Records Management, Digital Signature Platform, and other enterprise applications while providing role-based security, workflow automation, notifications, audit trails, and complete traceability of all project portfolio activities.		

2.2.4.2.1.9 Safety Management

Ref / No.	Process / Requirement	Tenderers Response (Yes/No)	Evidence Page
SHE01	**Process Safety, Electrical Safety, First Aid Box Audits and Effluent Monitoring**		
1	The system shall support planning, scheduling and execution of process safety, electrical safety and first aid box audits, and effluent monitoring.		
2	The system shall provide digital checklists and support the capture of audit and monitoring data and supporting evidence.		
3	The system shall generate, assign and track corrective actions, including reminders and escalation of overdue actions.		
4	The system shall provide dashboards and reports on audit findings, corrective actions and compliance.		
SHE02	**License Management**		
1	The system shall manage license types, eligibility requirements, applications and supporting documents.		
2	The system shall support license application submission, regulatory processing and fee payment tracking.		

3	The system shall securely store and distribute issued licenses and notify relevant stakeholders.		
SHE03	**Environmental and Social Impact Assessment (ESIA) License Management**		
1	The system shall manage ESIA project profiles, project classification and applicable assessment processes.		
2	The system shall manage ESIA auditors, audit teams, workflows and required documentation.		
3	The system shall support ESIA report submission, NEMA fee processing and payment tracking.		
4	The system shall securely store and distribute issued ESIA licenses to relevant stakeholders.		
SHE04	**Safety Observation and Corrective Actions (SOCA)**		
1	The system shall enable reporting and registration of safety observations and corrective actions, including supporting evidence.		
2	The system shall support assignment and notification of responsible BPOs and action owners.		
3	The system shall track corrective actions, evidence, review, verification and closure of SOCAs.		
SHE05	**Job Safety Analysis (JSA)**		
1	The system shall support identification of tasks, hazards, risks, affected persons and control measures.		
2	The system shall generate JSA matrices and support review, version control and digital approval.		
3	The system shall monitor JSA implementation and provide compliance and risk reporting.		
SHE06	**Incident Management**		
1	The system shall support incident reporting, notification and evidence capture.		
2	The system shall manage incident investigations, including evidence collection, findings and investigation reports.		
3	The system shall assign and track corrective actions and supporting evidence through to closure.		
4	The system shall manage Lessons from Incident and provide dashboards and reports on incidents and corrective action status.		
SHE07	**Hazardous Waste Management**		
1	The system shall support hazardous waste planning, identification, assessment and minimization.		
2	The system shall manage waste segregation, containment, storage, collection, transportation and related documentation.		
3	The system shall support hazardous waste emergency preparedness, response coordination and training.		
4	The system shall maintain hazardous waste records and support inspections, audits, incident investigations and corrective actions.		

2.2.4.2.1.10 Security Management

Code	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
SEC01	**Visitor Management**		
1.	The system shall provide centralized management of visitor registration, approval, access and tracking.		
2.	The system shall support visitor identification, pre-registration, check-in/check-out and occupancy monitoring.		
3.	The system shall support capture and verification of visitor identification details.		
4.	The system shall provide audit trails, role-based workflows, dashboards and reports for visitor management and security monitoring.		
SEC02	**Security Workforce Management**		
1.	The system shall support registration, onboarding, contract management, and maintenance of records for outsourced security service providers and hired security guards.		
2.	The system shall maintain centralized records of security guards including deployment locations, shifts, attendance, assignments, certifications, contracts, and payment terms.		
3.	The system shall support scheduling, assignment, attendance tracking, and deployment monitoring for hired security guards.		
4.	The system shall support automated generation, validation, approval, and tracking of payment requests for security service providers and hired guards based on approved attendance records, contracts, and service schedules.		
5.	The system shall integrate with finance and banking systems for payment processing, reconciliations, and statutory deductions where applicable.		
6.	The system shall support performance evaluations, incident logging, compliance tracking, and service quality assessments for security service providers and guards.		
7.	The system shall maintain comprehensive audit trails for deployments, attendance, approvals, payments, contracts, and user activities.		
8.	The system shall generate configurable security workforce reports and dashboards covering attendance, deployment status, overtime, contractor performance, payment status, incidents, and operational KPIs.		

Code	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
9.	The system shall support configurable workflows, role-based access, segregation of duties, audit trails, notifications, and report exports.		
SEC03	**Material Movement Management**		
1.	The system shall provide a centralized module for requesting, approving, tracking, and monitoring movement of materials, equipment, tools, and assets into and out of organizational premises.		
2.	The system shall support digital gate pass generation, approval workflows, movement permits, transfer requests, and authorization controls for plant and material movements.		
3.	The system shall support capture and validation of movement details including item descriptions, quantities, serial numbers, vehicle details, drivers, destinations, custodians, movement reasons, and supporting documentation.		
4.	The system shall support integration with inventory, warehouse, procurement, fleet, maintenance, finance, Enterprise Asset Management, and security systems through secure		
5.	The system shall support real-time check-in/check-out monitoring, movement verification, gate inspections, and automated discrepancy alerts for unauthorized or incomplete movements.		
6.	The system shall support automated notifications, escalation alerts, approval reminders, and movement status updates for security personnel, custodians, and authorized stakeholders.		
7.	The system shall maintain comprehensive audit trails for gate passes, approvals, inspections, movements, verifications, discrepancies, and user activities.		
8.	The system shall generate configurable movement management reports and dashboards covering plant movements, material transfers, pending approvals, discrepancies, unauthorized movements, and operational KPIs.		
9.	The system shall support configurable workflows, role-based access, segregation of duties, audit trails, notifications, and report exports.		
SEC04	**Seal Management**		
1.	The system shall maintain a central register of seal serial numbers, seal type, status, station/location and other relevant seal attributes.		
2.	The system shall allow the issuance of seals from the available inventory.		

Code	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
3.	The system shall support controlled transfer of seals from one station to another.		
4.	The system shall link an issued seal to the relevant installation, asset, facility or location.		
5.	The system shall allow authorized Security personnel to flag a seal as Damaged, missing or broken.		
6.	The system shall provide configurable alerts when seal stock at a station reaches or falls below a defined minimum level.		
7.	The system shall allow an authorized Security Officer to initiate an initial seal installation.		
8.	The system shall provide Seal Breaking and resealing Requisition with respective approvals and notifications.		
9.	The system shall provide operational and management reports covering seal inventory, installations, seal breaking, resealing, broken seals, available seals, pending approvals, outstanding resealing, exceptions and transaction history.		
10.	The system shall integrate with HR, Material Master, Enterprise asset master, corporate authentication and the organisation's email.		

2.2.4.2.2 Sales and Commercial Management

2.2.4.2.2.1 Order Management

Overview

The proposed solution shall provide an integrated Order Management capability that supports the complete customer order lifecycle from order capture, validation, approval, scheduling, fulfilment, delivery, invoicing, and closure. The solution shall streamline order processing, improve customer service, optimize resource utilization, and provide real-time visibility into order status while integrating seamlessly with terminal operations, inventory management, customer management, pricing, billing, logistics, and financial management.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
OM01	Customer Order Capture	The solution shall support creation, submission, validation, amendment, cancellation, approval, and tracking of customer orders through multiple channels, including internal users, customer self-service portals, APIs, and other digital channels.		
OM02	Order Validation and Eligibility Management	The solution shall validate customer eligibility, contracts, credit limits, product availability, pricing, regulatory requirements, collateral arrangements, operational constraints, and business rules prior to order confirmation.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
OM03	Order Planning and Scheduling	The solution shall support order prioritization, allocation, scheduling, appointment management, resource allocation, loading schedules, delivery planning, and optimization of order fulfilment activities.		
OM04	Order Fulfilment Management	The solution shall support execution and monitoring of order fulfilment activities, including inventory allocation, product reservation, dispatch authorization, loading coordination, delivery confirmation, and order completion.		
OM05	Order Amendments and Exception Management	The solution shall support modification, suspension, cancellation, rescheduling, exception handling, dispute management, and resolution of order processing issues while maintaining complete audit trails.		
OM06	Order Tracking and Customer Visibility	The solution shall provide real-time visibility into order status, fulfilment progress, milestones, notifications, alerts, estimated completion times, and customer communications throughout the order lifecycle.		
OM07	Workflow and Approval Management	The solution shall support configurable workflows, delegated authority, approval processes, notifications, escalations, document attachments, and electronic approvals for order processing activities.		
OM08	Order Reporting and Analytics	The solution shall provide operational dashboards, order pipeline reporting, fulfilment performance, turnaround times, exception reporting, customer service metrics, trend analysis, executive dashboards, and self-service reporting with drill-down capabilities.		
OM09	Operational Compliance and Governance	The solution shall support configurable business rules, operational controls, segregation of duties, audit trails, transaction traceability, document management, and compliance with applicable organizational policies and regulatory requirements.		
OM10	Integration and Governance	The solution shall integrate seamlessly with Customer Management, Pricing Management, Billing & Revenue Management, Inventory Management, Terminal Management, Queue & Yard Management, Financial Management,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Customer Self-Service Portal, Enterprise Document & Records Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and complete traceability of all order management activities.		

2.2.4.2.2.2 Billing and Revenue Management

Overview

The proposed solution shall provide an integrated Billing & Revenue Management capability that supports the complete revenue lifecycle from charge calculation and invoice generation to revenue recognition, payment processing, collections, reconciliation, and financial reporting. The solution shall ensure accurate, timely, and transparent billing while supporting multiple pricing models, contractual agreements, statutory compliance, and seamless integration with operational and financial systems.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
BRM01	Billing Management	The solution shall support automated generation, validation, approval, adjustment, cancellation, and distribution of invoices, debit notes, credit notes, and other billing documents based on operational transactions, contracts, and pricing rules.		
BRM02	Tariff, Charges and Fee Management	The solution shall support configurable tariffs, transportation charges, storage charges, throughput fees, service charges, taxes, levies, discounts, penalties, and other commercial pricing components.		
BRM03	Revenue Recognition and Accounting	The solution shall support automated revenue recognition, accruals, deferred revenue, revenue adjustments, financial postings, and compliance with applicable accounting standards and organizational policies.		
BRM04	Payment Processing and Receipting	The solution shall support receipt processing, payment allocation, electronic payments, multiple payment methods, advance payments, deposits, customer account settlement, refunds, and payment reconciliation.		
BRM05	Credit and Collections Management	The solution shall support customer credit management, credit limits, ageing analysis, debt collection, overdue account management,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		payment reminders, dunning processes, write-offs, and recovery management.		
BRM06	Revenue Reconciliation	The solution shall support reconciliation of operational transactions, billing records, customer accounts, payments, banking transactions, and General Ledger postings to ensure financial accuracy and integrity.		
BRM07	Billing Workflow and Governance	The solution shall support configurable approval workflows, billing controls, delegated authority, exception handling, dispute management, audit trails, document attachments, and complete traceability of billing and revenue activities.		
BRM08	Billing and Revenue Reporting	The solution shall provide configurable billing reports, revenue dashboards, collections reports, ageing analysis, customer statements, profitability analysis, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
BRM09	Regulatory Compliance and Controls	The solution shall support statutory taxation, invoicing regulations, financial controls, audit requirements, electronic invoicing standards, and compliance with applicable regulatory and corporate governance requirements.		
BRM10	Integration and Governance	The solution shall integrate seamlessly with Order Management, Customer Management, Pricing Management, Financial Management, Terminal Management, Inventory Management, Customer Self-Service Portal, Enterprise Document & Records Management, banking platforms, taxation systems, and other enterprise applications while providing role-based security, workflow automation, notifications, and complete traceability of all billing and revenue management activities.		

2.2.4.2.2.3 Customer Account Management

Overview

The proposed solution shall provide an integrated Customer Account Management capability that supports the complete customer lifecycle from customer registration, onboarding, account administration, credit management, service management, and account maintenance to customer offboarding. The solution shall provide a single, centralized customer view while enabling efficient service delivery, regulatory compliance, and seamless integration with commercial, operational, and financial processes.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CAM01	Customer Registration and Onboarding	The solution shall support customer registration, onboarding, Know Your Customer (KYC) processes, customer classification, due diligence, account activation, and maintenance of complete customer master data.		
CAM02	Customer Master Data Management	The solution shall support creation, maintenance, validation, version control, and governance of customer profiles, contacts, locations, agreements, licenses, permits, and related master data.		
CAM03	Customer Account Administration	The solution shall support creation, maintenance, suspension, reactivation, closure, consolidation, and administration of customer accounts, including management of account hierarchies and multiple customer relationships.		
CAM04	Credit and Collateral Management	The solution shall support customer credit assessment, credit limits, collateral management, guarantees, securities, exposure monitoring, credit reviews, and enforcement of configurable credit policies.		
CAM05	Customer Service Management	The solution shall support management of customer requests, enquiries, account changes, service requests, approvals, correspondence, notifications, and customer communications throughout the customer lifecycle.		
CAM06	Customer Compliance Management	The solution shall support verification and monitoring of customer compliance with contractual obligations, regulatory requirements, licensing conditions, sanctions, and organizational policies.		
CAM07	Customer Relationship History	The solution shall maintain a complete history of customer interactions, transactions, contracts, communications, service requests, complaints, account changes, and operational activities to provide a 360-degree customer view.		
CAM08	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, audit trails, document attachments, and complete traceability of all customer account management activities.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CAM09	Customer Reporting and Analytics	The solution shall provide customer dashboards, account performance reports, customer segmentation, credit exposure reports, customer activity analysis, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
CAM10	Integration and Governance	The solution shall integrate seamlessly with Order Management, Billing & Revenue Management, Pricing Management, Customer Relationship Management, Customer Self-Service Portal, Financial Management, Contract Lifecycle Management, Enterprise Document & Records Management, Digital Signature Platform, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability.		

2.2.4.2.2.4 Pricing Management

Overview

The proposed solution shall provide an integrated Pricing Management capability that enables the Corporation to define, maintain, approve, and administer pricing structures for products and services. The solution shall support configurable tariff models, commercial agreements, regulatory pricing requirements, discounts, surcharges, taxes, and pricing simulations while ensuring consistency, transparency, and seamless integration with order management, billing, and financial processes.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
PM01	Tariff and Price Configuration	The solution shall support creation, maintenance, approval, and administration of tariffs, product prices, transportation charges, storage charges, throughput fees, service charges, and other commercial pricing structures.		
PM02	Pricing Rules and Policies	The solution shall support configurable pricing rules, pricing hierarchies, customer-specific pricing, contract pricing, volume-based pricing, promotional pricing, discounts, surcharges, penalties, and exemptions.		
PM03	Price Calculation and Validation	The solution shall automatically calculate applicable prices based on configurable business rules, customer agreements, products, quantities,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		locations, contracts, and operational transactions while validating pricing accuracy before billing.		
PM04	Pricing Approvals and Governance	The solution shall support configurable workflows for price creation, amendments, approvals, delegated authority, effective dating, version control, notifications, and complete audit trails for all pricing changes.		
PM05	Contract and Customer Pricing	The solution shall support management of customer-specific pricing agreements, negotiated tariffs, framework agreements, commercial contracts, special pricing arrangements, and contractual pricing obligations.		
PM06	Regulatory and Tax Pricing Compliance	The solution shall support application of statutory taxes, levies, regulatory tariffs, government pricing directives, and compliance with applicable pricing regulations and organizational policies.		
PM07	Pricing Simulation and Analysis	The solution shall support pricing simulations, scenario modelling, profitability analysis, impact assessment, tariff comparisons, revenue projections, and what-if analysis to support commercial decision-making.		
PM08	Pricing Reporting and Analytics	The solution shall provide configurable pricing dashboards, tariff reports, pricing history, discount analysis, profitability reports, pricing trend analysis, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
PM09	Pricing Controls and Auditability	The solution shall support role-based access control, segregation of duties, audit trails, change logs, exception management, document attachments, and complete traceability of all pricing activities.		
PM10	Integration and Governance	The solution shall integrate seamlessly with Customer Account Management, Order Management, Billing & Revenue Management, Commercial Contracts, Financial Management, Customer Self-Service Portal, and other enterprise applications while providing consistent pricing across all customer engagement channels and ensuring end-to-end governance.		

2.2.4.2.2.5 Commercial Contracts

Overview

The proposed solution shall provide an integrated Commercial Contracts capability to manage customer commercial agreements throughout their lifecycle, including contract initiation, negotiation, approval, execution, pricing administration, performance monitoring, amendments, renewals, and closure. The solution shall ensure that commercial transactions are governed by valid contractual agreements while supporting regulatory compliance, revenue assurance, and operational efficiency.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CC01	Commercial Contract Administration	The solution shall support creation, registration, negotiation, approval, execution, activation, amendment, renewal, suspension, termination, and archival of customer commercial contracts and agreements.		
CC02	Contract Templates and Clause Management	The solution shall support standardized contract templates, configurable clause libraries, commercial terms, pricing schedules, service levels, contractual obligations, and version control of contractual documents.		
CC03	Customer Agreement Management	The solution shall support management of transportation agreements, storage agreements, throughput agreements, service agreements, framework agreements, and other customer-specific commercial arrangements.		
CC04	Commercial Terms and Pricing Management	The solution shall support administration of contract-specific tariffs, pricing schedules, discounts, surcharges, rebates, penalties, incentives, taxation rules, and other commercial terms linked to customer agreements.		
CC05	Contract Performance and Obligation Management	The solution shall support monitoring of contractual obligations, service levels, milestones, deliverables, customer commitments, financial obligations, compliance requirements, and contract performance throughout the agreement lifecycle.		
CC06	Contract Change and Renewal Management	The solution shall support contract amendments, variations, extensions, renewals, expiry management, notifications, approval workflows, and complete auditability of contractual changes.		
CC07	Workflow and Governance	The solution shall support configurable workflows, delegated authority, legal reviews, approvals, notifications, escalations, document		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		attachments, electronic approvals, and complete traceability of all commercial contract activities.		
CC08	Commercial Contract Reporting and Analytics	The solution shall provide contract registers, expiry reports, obligation tracking, contract utilization reports, revenue forecasts, commercial performance dashboards, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
CC09	Compliance and Audit Management	The solution shall support compliance monitoring, audit trails, contract risk monitoring, document version control, access controls, exception management, and adherence to organizational policies and applicable regulatory requirements.		
CC10	Integration and Governance	The solution shall integrate seamlessly with Customer Account Management, Pricing Management, Order Management, Billing & Revenue Management, Financial Management, Customer Relationship Management, Enterprise Document & Records Management, Digital Signature Platform, and other enterprise applications while providing role-based security, workflow automation, notifications, and end-to-end governance of commercial contracts.		

2.2.4.2.2.6 Revenue Forecasting

Overview

The proposed solution shall provide an integrated Revenue Forecasting capability that enables the Corporation to forecast, monitor, and analyse revenue from all business operations. The solution shall support revenue planning, demand forecasting, sales projections, scenario modelling, profitability analysis, and variance monitoring to facilitate strategic decision-making, financial planning, and sustainable commercial growth.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
RF01	Revenue Planning and Forecasting	The solution shall support preparation of short-term, medium-term, and long-term revenue forecasts based on historical trends, customer demand, contracts, tariffs, operational capacity, and strategic business plans.		
RF02	Sales and Demand Forecasting	The solution shall support forecasting of product demand, transportation volumes, storage capacity utilization, customer		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		consumption patterns, market trends, and sales projections using configurable forecasting models.		
RF03	Revenue Scenario Modelling	The solution shall support scenario planning, sensitivity analysis, what-if simulations, tariff impact assessments, demand fluctuations, and market condition modelling to evaluate potential revenue outcomes.		
RF04	Profitability and Margin Analysis	The solution shall support analysis of revenue, costs, profitability, contribution margins, customer profitability, product profitability, route profitability, and business unit performance.		
RF05	Revenue Performance Monitoring	The solution shall support continuous monitoring of forecasted versus actual revenue, variance analysis, trend analysis, revenue leakage identification, and performance tracking against corporate targets.		
RF06	Revenue Risk Assessment	The solution shall support identification, assessment, monitoring, and reporting of commercial risks that may affect revenue generation, including market risks, customer risks, operational constraints, and regulatory changes.		
RF07	Forecast Collaboration and Governance	The solution shall support collaborative forecasting, workflow-based reviews, approvals, version management, audit trails, notifications, delegated authority, and controlled publishing of revenue forecasts.		
RF08	Revenue Reporting and Analytics	The solution shall provide configurable revenue dashboards, forecasting reports, variance reports, profitability reports, executive dashboards, KPI monitoring, predictive analytics, and self-service reporting with drill-down capabilities.		
RF09	Forecast Data Management	The solution shall support consolidation, validation, version control, and governance of forecasting data from operational, commercial, financial, and external market sources to ensure forecast accuracy and consistency.		
RF10	Integration and Governance	The solution shall integrate seamlessly with Strategic Planning & Performance Management, Budgeting & Planning, Customer Account Management, Pricing Management, Order Management, Billing & Revenue Management, Financial Management, Business Intelligence, and other enterprise applications while providing role-based security, workflow automation, notifications, audit trails, and complete traceability of all revenue forecasting activities.		

2.2.4.2.3 Stakeholder Management

2.2.4.2.3.1 Customer Relationship Management (CRM)

Overview

The proposed solution shall provide an integrated Customer Relationship Management (CRM) capability that enables the Corporation to effectively manage customer relationships throughout the customer lifecycle. The solution shall support customer engagement, sales opportunities, service requests, communications, account management, stakeholder interactions, and customer

insights while providing a unified 360-degree customer view to enhance customer experience, service delivery, and business growth.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CRM01	Customer Profile Management	The solution shall support centralized management of customer profiles, customer segmentation, contacts, organizations, stakeholder relationships, communication preferences, interaction history, and customer master information.		
CRM02	Customer Engagement Management	The solution shall support planning, execution, and monitoring of customer engagements, meetings, visits, campaigns, relationship activities, and stakeholder interactions across multiple communication channels.		
CRM03	Opportunity and Pipeline Management	The solution shall support identification, qualification, tracking, prioritization, and management of business opportunities, customer leads, commercial engagements, and sales pipelines from initiation to closure.		
CRM04	Customer Service and Request Management	The solution shall support management of customer enquiries, service requests, requests for information, account support, escalations, follow-ups, and resolution tracking through configurable workflows.		
CRM05	Customer Communication Management	The solution shall support management of customer correspondence, notifications, emails, SMS, letters, meetings, announcements, communication history, and omnichannel engagement.		
CRM06	Customer Satisfaction and Feedback Management	The solution shall support customer satisfaction surveys, feedback collection, service quality monitoring, customer experience measurement, sentiment analysis, and continuous improvement initiatives.		
CRM07	Customer Collaboration and Self-Service Integration	The solution shall support secure collaboration with customers through customer portals, self-service capabilities, electronic document exchange, workflow notifications, and digital communication channels.		
CRM08	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, audit trails, document attachments, and complete traceability of all customer relationship management activities.		
CRM09	Customer Reporting and Analytics	The solution shall provide customer dashboards, customer segmentation reports, customer engagement reports, service performance metrics, opportunity analysis, customer satisfaction reports, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CRM10	Integration and Governance	The solution shall integrate seamlessly with Customer Account Management, Order Management, Commercial Contracts, Billing & Revenue Management, Customer Self-Service Portal, Communications Management, Case Management, Complaint Management, Enterprise Document & Records Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability.		

2.2.4.2.3.2 Supplier Relationship Management (SRM)

Overview

The proposed solution shall provide an integrated Supplier Relationship Management (SRM) capability that supports the complete supplier lifecycle from supplier registration, qualification, onboarding, performance management, collaboration, contract engagement, and continuous evaluation. The solution shall promote strategic supplier partnerships, enhance procurement efficiency, improve supplier performance, strengthen compliance, and provide a single source of supplier information across the Corporation.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
SRM01	Supplier Registration and Onboarding	The solution shall support supplier self-registration, qualification, prequalification, onboarding, categorization, due diligence, document verification, approval workflows, and supplier master data management.		
SRM02	Supplier Master Data Management	The solution shall support centralized management of supplier profiles, contacts, certifications, licences, tax information, banking details, product and service categories, and supplier lifecycle management.		
SRM03	Supplier Qualification and Compliance	The solution shall support supplier evaluation, compliance verification, risk assessments, statutory compliance monitoring, certification management, blacklisting, suspension, reinstatement, and ongoing supplier qualification.		
SRM04	Supplier Performance Management	The solution shall support supplier performance evaluation using configurable KPIs, service level agreements (SLAs), quality metrics, delivery performance, contract compliance, scorecards, and continuous improvement initiatives.		
SRM05	Supplier Collaboration and Communication	The solution shall support secure collaboration with suppliers through supplier portals, electronic document exchange, notifications, enquiries, clarifications, meetings, correspondence management, and workflow-based communications.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
SRM06	Supplier Risk and Relationship Management	The solution shall support identification, monitoring, and mitigation of supplier risks, relationship management, strategic supplier segmentation, supplier development programmes, dispute management, and business continuity planning.		
SRM07	Supplier Self-Service	The solution shall provide suppliers with secure self-service capabilities to manage organizational information, submit statutory documents, respond to procurement opportunities, monitor contract performance, track transactions, and receive notifications.		
SRM08	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, audit trails, document attachments, and complete traceability of all supplier relationship management activities.		
SRM09	Supplier Reporting and Analytics	The solution shall provide supplier dashboards, supplier performance reports, supplier compliance reports, spend analysis, supplier risk reports, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
SRM10	Integration and Governance	The solution shall integrate seamlessly with Supply Chain & Electronic Procurement, Contract Lifecycle Management, Financial Management, Enterprise Asset Management, Enterprise Document & Records Management, Digital Signature Platform, Governance, Risk & Compliance, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of supplier relationship management activities.		

2.2.4.2.3.3 Marketing and Campaign Management

Overview

The proposed solution shall provide an integrated Marketing & Campaign Management capability that enables the Corporation to plan, execute, monitor, and evaluate marketing initiatives, stakeholder engagement programmes, public awareness campaigns, customer outreach, and brand management activities. The solution shall support multi-channel campaign execution, audience segmentation, performance measurement, and analytics to enhance customer acquisition, retention, and stakeholder engagement.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MCM01	Marketing Strategy and Campaign Planning	The solution shall support planning, budgeting, scheduling, approval, and management of marketing campaigns, promotional activities, stakeholder engagement initiatives, and corporate communication programmes.		
MCM02	Audience and Market Segmentation	The solution shall support segmentation of customers and stakeholders based on configurable demographic, geographic, behavioural, commercial, and operational criteria to facilitate targeted campaigns and communications.		
MCM03	Campaign Execution Management	The solution shall support execution of marketing campaigns across multiple communication channels, including email, SMS, web portals, social media, mobile applications, and other digital platforms.		
MCM04	Content and Brand Management	The solution shall support creation, approval, storage, publication, and lifecycle management of marketing content, promotional materials, branding assets, corporate publications, and campaign documentation.		
MCM05	Lead and Opportunity Generation	The solution shall support identification, capture, qualification, assignment, tracking, and conversion of business leads and commercial opportunities generated through marketing and stakeholder engagement activities.		
MCM06	Campaign Performance Monitoring	The solution shall support monitoring of campaign execution, customer participation, engagement levels, conversion rates, campaign effectiveness, return on investment (ROI), and achievement of campaign objectives.		
MCM07	Workflow and Governance	The solution shall support configurable workflows for campaign planning, approvals, content review, publication, notifications, escalations, delegated authority, audit trails, and document management throughout the campaign lifecycle.		
MCM08	Marketing Reporting and Analytics	The solution shall provide configurable dashboards, campaign performance reports, customer engagement analytics, lead conversion reports, marketing ROI analysis, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
MCM09	Marketing Compliance and Governance	The solution shall support compliance with corporate branding standards, communication policies, regulatory requirements, consent management, auditability, and secure management of marketing information and stakeholder data.		
MCM10	Integration and Governance	The solution shall integrate seamlessly with Customer Relationship Management, Customer Account Management, Communications Management,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Customer Self-Service Portal, Enterprise Document & Records Management, Business Intelligence, and other enterprise applications while providing role-based security, workflow automation, notifications, audit trails, and complete traceability of all marketing and campaign management activities.		

2.2.4.2.3.4 Communications Management

Overview

The proposed solution shall provide an integrated Communications Management capability that enables the Corporation to plan, manage, deliver, monitor, and archive internal and external communications across multiple channels. The solution shall support stakeholder engagement, corporate communications, operational notifications, regulatory communications, crisis communications, and collaboration while ensuring consistency, governance, and timely dissemination of information.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
COM01	Corporate Communications Management	The solution shall support planning, creation, approval, publication, distribution, and management of corporate announcements, notices, circulars, newsletters, press releases, and official communications.		
COM02	Multi-Channel Communication	The solution shall support communication through multiple channels, including email, SMS, mobile applications, web portals, instant messaging, social media, digital signage, and other communication platforms.		
COM03	Stakeholder Engagement Management	The solution shall support planning, coordination, execution, and tracking of communications with customers, suppliers, regulators, government agencies, employees, and other stakeholders.		
COM04	Notification and Alert Management	The solution shall support configurable automated notifications, reminders, operational alerts, escalations, broadcast messages, and event-driven communications based on configurable business rules and workflows.		
COM05	Correspondence Management	The solution shall support creation, receipt, routing, tracking, approval, storage, and archival of official correspondence, including letters, emails, memoranda, and other communication records.		
COM06	Crisis and Emergency Communications	The solution shall support rapid dissemination of emergency notifications, incident communications, crisis management messaging, business continuity communications, and stakeholder updates during operational disruptions.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
COM07	Workflow and Governance	The solution shall support configurable workflows for communication review, approvals, publication, distribution, notifications, delegated authority, audit trails, document attachments, and complete traceability of communication activities.		
COM08	Communications Reporting and Analytics	The solution shall provide communication dashboards, delivery reports, stakeholder engagement metrics, communication effectiveness analysis, notification status, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
COM09	Communication Compliance and Records Management	The solution shall support communication retention policies, document version control, regulatory compliance, communication audit trails, records management, access controls, and preservation of official communication records.		
COM10	Integration and Governance	The solution shall integrate seamlessly with Customer Relationship Management, Supplier Relationship Management, Case Management, Complaint Management, Enterprise Document & Records Management, Digital Signature Platform, Marketing & Campaign Management, IT Service Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all communication activities.		

2.2.4.2.3.5 Complaint Management

Overview

The proposed solution shall provide an integrated Complaint Management capability to enable the Corporation to receive, register, investigate, resolve, monitor, and report customer, supplier, employee, and stakeholder complaints. The solution shall support standardized complaint handling processes, service level management, regulatory compliance, root cause analysis, continuous improvement, and transparent communication throughout the complaint lifecycle.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CPM01	Complaint Registration and Intake	The solution shall support receipt, registration, categorization, prioritization, acknowledgement, and tracking of complaints received through multiple channels, including customer portals, email,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		telephone, mobile applications, APIs, and walk-in channels.		
CPM02	Complaint Assessment and Assignment	The solution shall support complaint classification, impact assessment, routing, assignment, workload balancing, ownership management, and prioritization using configurable business rules and workflows.		
CPM03	Investigation and Resolution Management	The solution shall support investigation, evidence collection, collaboration, root cause analysis, corrective actions, approvals, resolution tracking, and closure of complaints while maintaining complete case histories.		
CPM04	Complaint Communication and Stakeholder Engagement	The solution shall support automated acknowledgements, status notifications, correspondence management, stakeholder communications, feedback requests, escalation notifications, and communication history throughout the complaint lifecycle.		
CPM05	Service Level and Escalation Management	The solution shall support configurable service level agreements (SLAs), response timelines, escalation rules, reminders, overdue monitoring, exception handling, and performance monitoring against established service standards.		
CPM06	Corrective and Preventive Action Management	The solution shall support recording, assignment, implementation, monitoring, verification, and closure of corrective and preventive actions arising from complaint investigations to facilitate continuous service improvement.		
CPM07	Complaint Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, audit trails, document attachments, records retention, and complete traceability of all complaint management activities.		
CPM08	Complaint Reporting and Analytics	The solution shall provide configurable dashboards, complaint trend analysis, root cause analysis, SLA performance reports, complaint resolution metrics, customer satisfaction reports, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
CPM09	Compliance and Audit Management	The solution shall support compliance with regulatory requirements, organizational policies, records management standards, audit requirements, data privacy obligations, and complete auditability of complaint handling activities.		
CPM10	Integration and Governance	The solution shall integrate seamlessly with Customer Relationship Management, Customer Account Management, Case Management, Communications Management, Enterprise Document & Records		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Management, Digital Signature Platform, Governance, Risk & Compliance, Business Intelligence, Customer Self-Service Portal, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all complaint management activities.		

2.2.4.2.4 Enterprise Asset Management

2.2.4.2.4.1 Maintenance Management

Overview

The proposed solution shall provide an integrated Maintenance Management capability to support the planning, scheduling, execution, monitoring, and optimization of preventive, predictive, corrective, and emergency maintenance activities across the Corporation's pipeline network, terminals, depots, facilities, plant, equipment, vehicles, and supporting infrastructure. The solution shall improve asset availability, operational reliability, maintenance efficiency, regulatory compliance, and lifecycle cost management.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MM01	Maintenance Planning and Scheduling	The solution shall support planning, scheduling, prioritization, forecasting, and coordination of preventive, predictive, corrective, condition-based, and emergency maintenance activities using configurable maintenance strategies and calendars.		
MM02	Work Order Management	The solution shall support creation, approval, assignment, execution, monitoring, suspension, completion, and closure of maintenance work orders, including labour, materials, equipment, contractor management, and cost tracking.		
MM03	Preventive and Predictive Maintenance	The solution shall support time-based, usage-based, condition-based, and predictive maintenance programmes, including automated maintenance scheduling, equipment health monitoring, inspections, and maintenance optimization.		
MM04	Inspection and Condition Monitoring	The solution shall support routine inspections, condition assessments, defect identification, equipment monitoring, asset health evaluations, inspection checklists, and recording of inspection findings and recommendations.		
MM05	Resource and Maintenance Execution Management	The solution shall support planning and allocation of maintenance personnel, contractors, tools, equipment, spare parts, permits, and other resources required for efficient execution of maintenance activities.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MM06	Maintenance Cost and Performance Management	The solution shall support maintenance budgeting, cost tracking, labour costing, material consumption, contractor costs, maintenance history, equipment downtime analysis, KPIs, and lifecycle cost analysis.		
MM07	Maintenance Compliance and Safety	The solution shall support permit-to-work integration, safety procedures, isolation management, work instructions, regulatory inspections, environmental compliance, quality assurance, audit trails, and adherence to maintenance standards and statutory requirements.		
MM08	Maintenance Reporting and Analytics	The solution shall provide configurable dashboards, maintenance schedules, work order status, equipment downtime reports, backlog analysis, maintenance cost reports, asset performance metrics, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
MM09	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, document attachments, electronic records, audit trails, and complete traceability of all maintenance management activities.		
MM10	Integration and Governance	The solution shall integrate seamlessly with Asset Integrity Management, Work Management, Maintenance Inventory Management, Field Services Management, Project Portfolio Management, Financial Management, Supply Chain & Electronic Procurement, Enterprise Document & Records Management, Digital Signature Platform, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all maintenance activities.		

2.2.4.2.4.2 Asset Integrity Management

Overview

The proposed solution shall provide an integrated Asset Integrity Management capability to support the inspection, monitoring, assessment, protection, and lifecycle management of the Corporation's critical assets. The solution shall enable proactive management of asset health, integrity risks, regulatory compliance, reliability, and operational safety across pipelines, terminals, depots, facilities, mechanical equipment, electrical systems, instrumentation, and associated infrastructure.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
AIM01	Asset Integrity Planning	The solution shall support development, execution, monitoring, and continuous		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		improvement of asset integrity programmes, inspection plans, integrity strategies, maintenance philosophies, and risk-based inspection schedules throughout the asset lifecycle.		
AIM02	Asset Health and Condition Monitoring	The solution shall support continuous monitoring of asset condition, health indices, performance parameters, degradation trends, equipment diagnostics, and condition-based maintenance using configurable monitoring techniques and inspection data.		
AIM03	Inspection and Integrity Assessment	The solution shall support planning, execution, recording, and analysis of integrity inspections, non-destructive testing (NDT), corrosion monitoring, thickness measurements, pressure testing, fitness-for-service assessments, and integrity evaluations.		
AIM04	Defect and Anomaly Management	The solution shall support identification, classification, risk assessment, investigation, prioritization, monitoring, and resolution of defects, anomalies, failures, corrosion findings, leaks, and integrity threats affecting critical assets.		
AIM05	Integrity Risk Management	The solution shall support identification, assessment, mitigation, monitoring, and reporting of integrity risks using configurable risk models, consequence analysis, likelihood assessments, risk matrices, and mitigation planning.		
AIM06	Regulatory Compliance and Integrity Assurance	The solution shall support compliance with applicable engineering standards, statutory inspection requirements, environmental regulations, safety requirements, and integrity management policies through automated monitoring, alerts, and audit trails.		
AIM07	Asset Lifecycle and Performance Management	The solution shall support lifecycle assessment, remaining useful life estimation, refurbishment planning, replacement planning, asset criticality analysis, integrity performance measurement, and investment prioritization.		
AIM08	Asset Integrity Reporting and Analytics	The solution shall provide configurable dashboards, integrity status reports, corrosion analysis, inspection performance reports, asset		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		health dashboards, integrity KPIs, executive dashboards, predictive analytics, and self-service reporting with drill-down capabilities.		
AIM09	Workflow and Governance	The solution shall support configurable workflows, engineering approvals, delegated authority, notifications, corrective action tracking, document attachments, audit trails, and complete traceability of all asset integrity management activities.		
AIM10	Integration and Governance	The solution shall integrate seamlessly with Maintenance Management, Reliability & Asset Performance Management, Work Management, Field Services Management, Project Portfolio Management, Enterprise Document & Records Management, GIS, SCADA, IoT platforms, Financial Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all asset integrity activities.		

2.2.4.2.4.3 Work Management

Overview

The proposed solution shall provide an integrated Work Management capability to support the planning, authorization, execution, monitoring, and completion of operational and maintenance work across the Corporation's assets and facilities. The solution shall optimize workforce productivity, improve resource utilization, enforce operational controls, and ensure safe, compliant, and efficient execution of planned and unplanned work.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
WM01	Work Planning and Scheduling	The solution shall support planning, prioritization, scheduling, rescheduling, and coordination of operational and maintenance work using configurable work calendars, resource availability, and business priorities.		
WM02	Work Request and Work Order Management	The solution shall support creation, approval, assignment, execution, monitoring, suspension, completion, and closure of work requests and work orders while maintaining complete work histories and audit trails.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
WM03	Resource Planning and Allocation	The solution shall support planning, allocation, scheduling, and optimization of personnel, contractors, equipment, tools, vehicles, materials, and other resources required for execution of work activities.		
WM04	Permit-to-Work and Operational Safety	The solution shall support electronic permit-to-work processes, isolation management, lockout/tagout procedures, safety checklists, hazard identification, risk assessments, work authorizations, and compliance with operational safety procedures.		
WM05	Task Execution and Progress Monitoring	The solution shall support execution, progress tracking, milestone monitoring, completion verification, field updates, issue management, corrective actions, and real-time visibility into work execution status.		
WM06	Labour, Material and Cost Management	The solution shall support recording and monitoring of labour hours, contractor effort, material consumption, equipment utilization, service costs, and overall work execution costs for performance and financial analysis.		
WM07	Document and Technical Information Management	The solution shall support attachment and management of engineering drawings, standard operating procedures, inspection reports, manuals, permits, photographs, checklists, and other work-related documentation.		
WM08	Work Performance Reporting and Analytics	The solution shall provide configurable dashboards, work order status reports, backlog analysis, workforce productivity reports, resource utilization, SLA compliance, cost analysis, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
WM09	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, audit trails, document attachments, electronic records, and complete traceability of all work management activities.		
WM10	Integration and Governance	The solution shall integrate seamlessly with Maintenance Management, Asset Integrity Management, Field Services Management, Maintenance Inventory Management, Project Portfolio Management, Financial Management, Supply Chain & Electronic Procurement, Enterprise Document & Records Management, GIS, SCADA, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all work management activities.		

2.2.4.2.4.4 Field Services Management

Overview

The proposed solution shall provide an integrated Field Services Management capability to support the planning, dispatch, execution, monitoring, and optimization of field operations performed by

employees, contractors, and service providers. The solution shall enable mobile workforce management, real-time field visibility, improved resource utilization, enhanced operational safety, and timely completion of field activities while integrating seamlessly with maintenance, work management, asset management, and enterprise business processes.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
FSM01	Field Workforce Planning and Scheduling	The solution shall support planning, scheduling, dispatching, rescheduling, and optimization of field personnel, contractors, equipment, and vehicles based on skills, availability, location, workload, and operational priorities.		
FSM02	Mobile Work Execution	The solution shall provide secure mobile capabilities for field personnel to receive work assignments, update work progress, capture field data, record labour and material consumption, complete inspections, and close assigned tasks in both online and offline modes.		
FSM03	Dispatch and Resource Coordination	The solution shall support real-time dispatching, resource allocation, route optimization, workload balancing, emergency work assignments, and monitoring of field activities from centralized control centres.		
FSM04	Inspection and Field Data Capture	The solution shall support field inspections, condition assessments, digital checklists, measurements, photographs, videos, GPS coordinates, electronic forms, and collection of operational data from field activities.		
FSM05	Health, Safety and Environmental Compliance	The solution shall support field safety procedures, permit-to-work verification, risk assessments, toolbox talks, incident reporting, personal protective equipment (PPE) compliance, environmental monitoring, and regulatory compliance during field operations.		
FSM06	Field Asset and Inventory Management	The solution shall support tracking and utilization of field equipment, tools, spare parts, consumables, vehicles, and mobile inventory required for execution of field activities.		
FSM07	Collaboration and Communication	The solution shall support real-time communication between field teams and control centres through messaging, notifications, document sharing, work instructions, escalation workflows, and collaboration tools to improve operational coordination.		
FSM08	Field Performance Reporting and Analytics	The solution shall provide configurable dashboards, workforce productivity reports, field activity status, travel analysis, SLA performance, inspection reports, executive dashboards, KPI monitoring, geospatial		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		reporting, and self-service reporting with drill-down capabilities.		
FSM09	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, escalations, audit trails, document attachments, electronic records, and complete traceability of all field service management activities.		
FSM10	Integration and Governance	The solution shall integrate seamlessly with Work Management, Maintenance Management, Asset Integrity Management, Maintenance Inventory Management, GIS, SCADA, IoT platforms, Enterprise Document & Records Management, Financial Management, Human Capital & Payroll Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all field service activities.		

2.2.4.2.4.5 Maintenance Inventory Management

Overview

The proposed solution shall provide an integrated Maintenance Inventory Management capability to support the planning, procurement, storage, tracking, replenishment, and issuance of spare parts, maintenance materials, tools, consumables, and repair components required for maintenance and operational activities. The solution shall optimize inventory levels, improve material availability, reduce stockholding costs, and ensure seamless integration with maintenance, procurement, warehouse, and financial processes.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MIM01	Spare Parts and Maintenance Materials Management	The solution shall support centralized management of spare parts, consumables, repair materials, maintenance kits, tools, and equipment, including item classification, specifications, serialization, batching, and lifecycle management.		
MIM02	Inventory Planning and Replenishment	The solution shall support demand forecasting, minimum and maximum stock levels, reorder points, safety stock calculations, automated replenishment, procurement planning, and inventory optimization		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		based on maintenance requirements and consumption trends.		
MIM03	Warehouse and Stock Operations	The solution shall support goods receipt, inspection, storage, bin management, stock transfers, reservations, picking, issuing, returns, stock adjustments, cycle counting, and physical inventory verification across multiple warehouses and maintenance stores.		
MIM04	Material Reservation and Issue Management	The solution shall support reservation, allocation, issuance, return, and consumption of materials against maintenance work orders, projects, inspections, and operational activities while maintaining complete material traceability.		
MIM05	Inventory Traceability and Asset Association	The solution shall support end-to-end traceability of spare parts and maintenance materials, including serial numbers, batch numbers, shelf life, warranty tracking, asset associations, and maintenance history.		
QC09	Laboratory Equipment & Competency	The solution shall support management of laboratory equipment and personnel competency, including equipment inventory, calibration, verification, maintenance, qualification, malfunction management, service history, analyst qualifications, training, certification, and authorization to perform specified tests.		
MIM06	Inventory Cost and Valuation Management	The solution shall support inventory valuation, standard and moving average costing, stock adjustments, material consumption costing, obsolete inventory management, and financial reconciliation with the General Ledger.		
MIM07	Inventory Performance and Optimization	The solution shall support monitoring of inventory turnover, stock ageing, stock-outs, excess inventory, slow-moving items, critical spares, warehouse utilization, and optimization through configurable KPIs and alerts.		
MIM08	Inventory Reporting and Analytics	The solution shall provide configurable dashboards, inventory valuation reports, stock availability reports, consumption analysis, replenishment reports, warehouse performance dashboards, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
MIM09	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, audit trails, document attachments, segregation of duties, inventory controls, and complete traceability of all maintenance inventory activities.		
MIM10	Integration and Governance	The solution shall integrate seamlessly with Maintenance Management, Work Management, Field Services Management, Supply Chain & Electronic		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		Procurement, Financial Management, Enterprise Asset Management, Enterprise Document & Records Management, and other enterprise applications while providing role-based security, workflow automation, notifications, and comprehensive auditability of all maintenance inventory management activities.		

2.2.4.2.4.6 Reliability and Asset Performance Management

Overview

The proposed solution shall provide an integrated Reliability & Asset Performance Management capability to optimize the reliability, availability, maintainability, and performance of the Corporation's assets throughout their lifecycle. The solution shall support asset performance monitoring, reliability engineering, predictive analytics, failure analysis, risk-based decision-making, and continuous improvement to maximize asset value, minimize downtime, and improve operational efficiency.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
RAPM01	Asset Reliability Management	The solution shall support development, implementation, monitoring, and continuous improvement of asset reliability strategies, reliability programmes, maintenance optimization initiatives, and asset lifecycle performance management.		
RAPM02	Asset Performance Monitoring	The solution shall support continuous monitoring of asset availability, utilization, efficiency, throughput, operating conditions, health indicators, and performance against defined operational targets and service levels.		
RAPM03	Failure Analysis and Root Cause Management	The solution shall support recording, investigation, analysis, and reporting of equipment failures, recurring defects, root causes, corrective actions, preventive actions, and lessons learned to improve asset reliability.		
RAPM04	Predictive Analytics and Condition-Based Maintenance	The solution shall support predictive maintenance models, condition monitoring, trend analysis, anomaly detection, remaining useful life estimation, and AI-driven recommendations for maintenance planning and asset optimization.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
RAPM05	Reliability Engineering and Risk Assessment	The solution shall support reliability engineering methodologies, criticality assessments, Failure Modes and Effects Analysis (FMEA), Reliability-Centred Maintenance (RCM), risk-based maintenance, and asset performance optimization.		
RAPM06	Asset Lifecycle Optimization	The solution shall support lifecycle costing, refurbishment planning, replacement planning, asset investment analysis, capital renewal planning, performance benchmarking, and optimization of asset lifecycle decisions.		
RAPM07	Performance Benchmarking and Continuous Improvement	The solution shall support benchmarking of asset performance, maintenance effectiveness, operational efficiency, industry best practices, continuous improvement initiatives, and performance optimization programmes.		
RAPM08	Reliability Reporting and Analytics	The solution shall provide configurable dashboards, asset health reports, reliability KPIs, Mean Time Between Failures (MTBF), Mean Time to Repair (MTTR), availability reports, performance trends, predictive analytics, executive dashboards, and self-service reporting with drill-down capabilities.		
RAPM09	Workflow and Governance	The solution shall support configurable workflows, engineering reviews, approvals, notifications, audit trails, corrective action tracking, document attachments, electronic records, and complete traceability of all reliability and asset performance management activities.		
RAPM10	Integration and Governance	The solution shall integrate seamlessly with Asset Integrity Management, Maintenance Management, Work Management, Field Services Management, SCADA, GIS, IoT platforms, Enterprise Monitoring & Observability, AI, Analytics & Enterprise Reporting, Financial Management, and other enterprise applications while providing role-based security, workflow automation,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		notifications, and comprehensive auditability of all reliability and asset performance management activities.		

2.2.4.2.5 Cross-Cutting Enterprise Services

2.2.4.2.5.1 Information Security Functionality

Overview

The Information Security Functionality aims to ensure that the ERP solution is designed, implemented, integrated, and operated within a secure, resilient, compliant, and scalable environment based on security-by-design and security-by-default principles. The solution shall provide centralized Identity and Access Management (IAM) incorporating RBAC, SSO, MFA and identity federation; robust Privileged Access Management (PAM); encryption and enterprise key management; centralized logging, SIEM, monitoring and threat detection; and comprehensive protection for applications, endpoints, containers and other workloads. It shall further ensure secure segregation and controlled integration of OT environments, secure communications and system integrations, continuous security and compliance monitoring, comprehensive audit trails and governance reporting, and centralized enterprise-wide visibility of security risks and events. The security architecture shall be scalable and adaptable to emerging threats, technologies, regulatory requirements and future business needs throughout the Digital Transformation program.

4. Functional requirements

The proposed solution should meet functional requirements and are provided in the tables below.

Code	Functional Area	Requirement Description	Tenderers Response (Yes/No)	Evidence Page
ISR01	**Role-Based Access Control (RBAC)**	The solution shall provide a centralized and governed Role-Based Access Control (RBAC) framework that manages user access through reusable business, technical, composite, and hierarchical roles aligned with organizational structures, job functions, responsibilities, and business processes. Business roles shall remain independent of technical authorizations, have designated business owners, support organizational variations, and be reusable across departments, while centrally maintained technical roles shall define access to transactions, applications, APIs, reports, workflows, dashboards, authorization objects, and administrative functions. The solution shall support configurable and auditable role inheritance, role-to-organizational-unit assignments, and workflows for requesting and approving role assignments, while minimizing direct permission assignments through controlled exception processes and providing enhanced governance for privileged roles.		
ISR02	**Business Roles and Technical Roles**	The solution should provide comprehensive Business and Technical Role Management capabilities that enable creation of business roles aligned with organizational job functions while maintaining clear separation from the underlying technical permissions covering		

Code	Functional Area	Requirement Description	Tenderers Response (Yes/No)	Evidence Page
		transactions, applications, APIs, reports, workflows, authorization objects, security profiles, menus, and mobile applications. It shall support **composite/grouped** and inherited roles, reuse of technical roles across multiple business roles, multiple concurrent role assignments, and organizational scoping based on attributes such as company, business unit, department, plant, warehouse, cost/profit centre, and country. The solution shall integrate with HR systems to enable attribute- and organizational-structure-based automated role assignment, resulting from employee movements and status changes. It shall further provide delegated role administration within authorized scopes, defined business, technical and security role ownership, centralized role catalogues, role version control and rollback, time-bound access with automatic expiry and renewal workflows, and role analytics to identify unused, duplicate and orphaned roles. All role lifecycle activities, including creation, modification, deletion, assignment, removal, approval, rejection, expiration and delegation, shall be fully auditable with comprehensive logs capturing relevant user, timestamp, source system, IP address and change information.		
ISR03	**Authorization Objects and Fine-Grained Access Control**	The solution shall provide a configurable authorization framework that controls access to business functions, transactions, applications, APIs, reports, business services, workflows, and dashboards. Access shall be evaluated using multiple criteria, including organizational attributes such as company, business unit, plant, warehouse, purchasing group, division, cost centre, profit centre, project, asset, customer, vendor, and material group. The solution shall control permitted activities such as display, create, change, delete, approve, reject, reverse, post, cancel, and print, and restrict access according to organizational structures. Workflow actions, including submission, approval, rejection, escalation, delegation, and cancellation, shall also be subject to authorization controls. The solution shall provide access simulation to identify effective and duplicate permissions, missing authorizations, Segregation of Duties (SoD) conflicts, and privileged access before assignment. It shall also support custom authorization objects for organization-specific applications,		

Code	Functional Area	Requirement Description	Tenderers Response (Yes/No)	Evidence Page
		extensions, APIs, reports, and integrations, and provide dashboards and analytics for excessive or unused permissions, high-risk access, privileged users, failed authorization attempts, authorization trends, and compliance status.		
ISR04	**Least Privilege Access Management**	The solution shall enforce the principle of least privilege, ensuring users receive only the access required to perform their approved duties. Access shall be based on business roles and attributes such as job title, position, department, business function, organizational unit, employment type, cost centre, and process ownership. Direct assignment of permissions shall be prohibited except through approved exceptions and shall be identified and reported. The solution shall minimize standing privileged access and support Just-in-Time (JIT) access, with appropriate approval, automatic expiry or revocation, and full activity logging. The solution shall automatically revoke or adjust access when employment ends or is suspended, responsibilities change, staff transfer, temporary assignments expire, contracts end, or third-party engagements conclude. It shall identify dormant accounts, inactive privileged accounts, unused roles and permissions, and obsolete service accounts. Service and non-human accounts shall follow the same access governance principles, including minimum permissions, secure credential management, defined ownership, usage monitoring, and periodic reviews. The solution shall continuously identify and recommend removal of excessive, duplicate, unused, obsolete, or conflicting access and maintain complete audit logs of access assignments, removals, privilege elevation, temporary access, privileged sessions, administrative overrides, and policy exceptions.		
ISR05	**Segregation of Duties (SoD) Management**	The solution shall provide an enterprise-wide Segregation of Duties (SoD) framework to identify conflicts across business functions, transactions, roles, authorization objects, APIs, workflows, and privileged activities. It shall maintain a configurable SoD rule library with industry-standard templates in English, organization-specific rules, risk classifications, version history, and change logs. SoD checks shall be performed before access is granted during role assignment, provisioning, access requests, temporary access, privilege elevation, and organizational transfers. Unacceptable		

Code	Functional Area	Requirement Description	Tenderers Response (Yes/No)	Evidence Page
		conflicts shall be prevented unless approved through a controlled exception process. The solution shall perform SoD analysis at user, business role, technical role, composite role, authorization object, transaction, API permission, and workflow levels. Identified conflicts shall be classified as Critical, High, Medium, or Low risk. Approved exceptions shall include business justification, risk assessment, duration, approver, risk owner, and compensating controls. The solution shall continuously monitor SoD conflicts, integrate SoD checks into access approval workflows, and provide dashboards showing conflicts, critical risks, outstanding remediation actions, approved exceptions, risk trends, and risk exposure by users, roles, and business units.		
ISR06	**Emergency Access Management**	The solution shall provide a dedicated Emergency Access Management framework for controlled and temporary privileged access. It shall support dedicated and uniquely identifiable emergency or Firefighter IDs, assigned to specific systems or business functions and governed to prevent their use for routine operations. The solution shall support Just-in-Time (JIT) privilege elevation and configurable request and approval workflows based on organizational policies. All emergency privileged sessions shall be monitored, including session start and end times, commands, transactions, reports, configuration changes, and administrative activities. The solution shall also provide Break-Glass access for critical outages or cyber incidents when normal identity services are unavailable, using predefined emergency accounts with immediate security alerts, complete audit trails, and mandatory post-event reviews. It shall integrate with PAM, Microsoft Active Directory, SIEM, and ITSM platforms and maintain comprehensive audit records for all emergency access activities.		
ISR07	**Role Mining and Role Engineering**	The solution shall provide automated role mining to analyze existing user access and recommend optimized role structures. It shall assess assigned permissions and actual system usage to identify frequently used, rarely used and unused permissions, common authorization combinations, shared business functions, and high-risk access combinations. The solution shall also provide role similarity analysis based		

Code	Functional Area	Requirement Description	Tenderers Response (Yes/No)	Evidence Page
		on common permissions, shared authorization objects, similar business functions, user populations, and transaction usage.		
ISR08	**Continuous Risk Analysis and Preventive Controls**	The solution shall provide a centralized and continuous risk analysis framework across all ERP modules and integrated enterprise systems without requiring manual execution. It shall assess every access request before approval based on business and technical roles, existing permissions, Segregation of Duties (SoD), least privilege, organizational scope, and risk scores. The solution shall continuously identify excessive, duplicate, obsolete, privileged, and high-risk permissions, as well as organizational and SoD conflicts before access is granted. The solution shall continuously monitor privileged users, administrative and service accounts, and emergency access sessions. It shall also assess API and integration risks, including excessive permissions, failed authentication, abnormal API activity, and unauthorized integrations. The solution should provide behavioral analytics to detect unusual user activities and generate configurable alerts. It shall provide dashboards for both executive and operational risk reporting.		
ISR09	**Authentication and Session Security**	The solution shall support single sign-on, multi-factor authentication and adaptive/risk-based authentication based on contextual signals such as device, location, and behaviour, together with configurable session timeout and concurrent-session controls.		

2.2.4.2.5.2 IT Service Management (ITSM)

Overview

IT Service Management (ITSM)

Overview

The proposed solution should provide an integrated IT Service Management (ITSM) capability that supports the planning, delivery, operation, monitoring, and continual improvement of ICT services in alignment with industry best practices such as ITIL. The solution shall enable efficient management of incidents, service requests, problems, changes, assets, configurations, service levels, knowledge, and service performance while supporting automation, self-service, and enterprise-wide governance.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
ITSM01	Service Desk and Request Management	The solution shall support a centralized service desk for logging, categorizing, prioritizing, routing, approving, fulfilling, monitoring, and closing incidents, service requests, enquiries, and ICT support requests through multiple communication channels.		
ITSM02	Incident and Problem Management	The solution shall support incident recording, classification, prioritization, escalation, root cause analysis, problem investigation, workaround management, known error management, and continual service improvement.		
ITSM03	Change and Release Management	The solution shall support planning, approval, scheduling, implementation, testing, deployment, rollback, and post-implementation review of changes, releases, patches, upgrades, and configuration updates using configurable workflows.		
ITSM04	Configuration and IT Asset Management	The solution shall support management of Configuration Items (CIs), Configuration Management Database (CMDB), ICT assets, software assets, licences, hardware inventory, asset lifecycle management, relationships, and dependency mapping.		
ITSM05	Service Catalogue and Service Level Management	The solution shall support management of service catalogues, service offerings, service requests, Service Level Agreements (SLAs), Operational Level Agreements (OLAs), performance monitoring, escalations, and service reporting.		
ITSM06	Knowledge Management	The solution shall support creation, approval, publication, version control, search, reuse, and lifecycle management of knowledge articles, standard operating procedures, troubleshooting guides, FAQs, and technical documentation.		
ITSM07	Self-Service and Workflow Automation	The solution shall provide configurable self-service portals, service request automation, approvals, notifications, chatbots, workflow orchestration, task		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		automation, and integration with digital communication channels.		
ITSM08	IT Service Reporting and Analytics	The solution shall provide configurable dashboards, incident reports, SLA compliance reports, service request analysis, asset utilization reports, service performance metrics, executive dashboards, KPI monitoring, trend analysis, and self-service reporting with drill-down capabilities.		
ITSM09	Governance, Compliance and Security	The solution shall support role-based access control, segregation of duties, audit trails, policy compliance, risk monitoring, approval workflows, electronic records management, and alignment with ICT governance and cybersecurity policies.		
ITSM10	Integration and Governance	The solution shall integrate seamlessly with Master & Reference Data Management, Enterprise Monitoring & Observability, Human Capital & Payroll Management, Enterprise Document & Records Management, Identity & Access Management, Financial Management, Governance, Risk & Compliance, AI, Analytics & Enterprise Reporting, and other enterprise applications while providing workflow automation, notifications, APIs, comprehensive auditability, and end-to-end service traceability.		

Technical Specifications

The following Technical Specifications/Terms of Reference define how each functional requirement above shall be technically realized and are provided in addition to the functional requirements as they were not addressed in the original specification.

Code	Technical Area	Technical Specification	Tenderer's Response YES/NO	Evidence Page
TS-ITSM01	Omni-Channel Service Desk	The solution shall support omni-channel ticket intake (self-service portal, email-		

Code	Technical Area	Technical Specification	Tenderer's Response YES/NO	Evidence Page
		to-case, phone/IVR, live chat, and mobile app), a configurable categorization and auto-routing engine, and SLA/OLA timers with automatic breach escalation, aligned to ITIL 4 practice guidance.		
TS-ITSM02	Incident, Problem and Major Incident Management	The solution shall support automated incident-to-problem linkage, structured root-cause-analysis templates (e.g., 5-Whys, Fishbone/Ishikawa), a searchable Known Error Database (KEDB), and a major-incident management workflow with war-room/bridge-call coordination and stakeholder communication automation.		
TS-ITSM03	Change, Release and Deployment Automation	The solution shall support Change Advisory Board (CAB) workflow automation, a change calendar with automated conflict/blackout-period detection, configurable risk/impact scoring, documented rollback procedures, and integration with CI/CD pipelines and release-automation tooling.		
TS-ITSM04	CMDB, Discovery and Asset Lifecycle	The solution shall provide a CMDB supporting agent-based and agentless auto-discovery, visual CI relationship/dependency mapping, software asset management with licence-compliance and entitlement tracking, barcode/RFID/QR-enabled hardware asset tracking, and integration with network/infrastructure discovery tools.		
TS-ITSM05	Service Catalogue and SLA Engine	The solution shall provide a configurable, multi-tier-approval service catalogue, automated SLA/OLA/underpinning-contract tracking with breach alerting, and optional service costing/chargeback and showback reporting.		
TS-ITSM06	Knowledge Base and KCS	The solution shall provide full-text and AI-assisted knowledge search, a version-controlled article lifecycle		

Code	Technical Area	Technical Specification	Tenderer's Response YES/NO	Evidence Page
		workflow, support for the Knowledge-Centered Service (KCS) methodology, and multi-language content management.		
TS-ITSM07	Automation, Chatbot and Orchestration	The solution shall provide an AI-powered virtual agent/chatbot for tier-0 self-service resolution, a low-code workflow-orchestration engine, integration hooks for Robotic Process Automation (RPA), and native mobile applications for iOS and Android.		
TS-ITSM08	Operational and Predictive Analytics	The solution shall provide embedded BI/analytics with real-time, NOC-style operational dashboards, automated SLA-compliance reporting, and predictive/AI-assisted analytics for incident-volume and trend forecasting.		
TS-ITSM09	Governance and Security Alignment	The solution shall enforce role-based and segregation-of-duties access control (integrated with the enterprise RBAC/IAM capability), maintain immutable audit logs of all service-management activity, and demonstrate alignment with ISO/IEC 20000, ITIL 4, and ISO/IEC 27001 control objectives.		
TS-ITSM10	Enterprise and ITOM Integration	The solution shall expose REST APIs and webhook-based event notifications, integrate with monitoring/observability and Application Performance Management (APM) tooling (e.g., via SNMP, syslog, or vendor APIs), support CMDB federation with IT Operations Management (ITOM) platforms, and support standard identity/integration protocols including SCIM, LDAP, and SAML.		

2.2.4.2.5.3 Enterprise Data Analytics and AI

Overview

The proposed solution should provide an integrated Enterprise Data Analytics and AI capability that enables the Corporation to collect, integrate, manage, govern, analyse, and derive actionable insights from enterprise data.

The solution should support enterprise business intelligence, advanced and predictive analytics, artificial intelligence, machine learning, Generative AI, data science, and AI-enabled decision support across the Corporation. The solution should provide a scalable, secure, and governed

analytical environment capable of integrating data from MSOOS, enterprise applications, operational technology, databases, files, APIs, and external data sources.
The solution should leverage the Corporation's existing Power BI platform for data visualization, dashboards, and self-service analytics and should provide trusted, governed, and analytics-ready data to Power BI without requiring replacement of the existing visualization platform.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
EDA01	**Enterprise Data Integration and Management**	The solution should support ingestion, integration, transformation, validation, consolidation, and management of structured, semi-structured, and unstructured data from MSOOS, enterprise applications, operational technology, databases, files, APIs, IoT devices, and approved external data sources.		
EDA02	**Enterprise Data Warehouse and Data Lake**	The solution should provide scalable enterprise data warehouse and data lake capabilities for centralized storage, historical retention, processing, and analysis of enterprise data, including structured, semi-structured, and unstructured data.		
EDA03	**Enterprise Business Intelligence and Reporting**	The solution should support enterprise business intelligence and reporting through operational, management, and executive reports, KPI reporting, trend analysis, scheduled reporting, exception reporting, drill-down analytics, and governed analytical datasets, with seamless integration with the Corporation's existing Power BI platform.		
EDA04	**Advanced and Predictive Analytics**	The solution should support statistical analysis, forecasting, predictive modelling, anomaly detection, trend analysis, scenario modelling, what-if analysis, optimization, and other advanced analytical techniques using historical, current, and, where applicable, real-time data.		
EDA05	**Artificial Intelligence and Machine Learning**	The solution should support development, training, testing, deployment, monitoring, and management of AI and machine learning models for prediction, classification, recommendation, anomaly detection, optimization, natural language processing, and other approved enterprise use cases.		

EDA06	**Generative AI and Intelligent Decision Support**	The solution should support approved Generative AI capabilities including natural-language interaction with enterprise information, intelligent search, summarization, document analysis, knowledge assistance, automated insight generation, and AI-assisted decision support, subject to applicable security, governance, privacy, and data protection requirements.		
EDA07	**Data Governance and Data Quality**	The solution should support enterprise data governance including data ownership, stewardship, classification, metadata management, data quality rules, validation, data lineage, master data alignment, data quality monitoring, data issue management, and controlled data lifecycle management.		
EDA08	**Real-Time and Operational Analytics**	The solution should support real-time and near-real-time data ingestion, processing, event detection, monitoring, alerts, and operational analytics for applicable enterprise and operational technology data sources.		
EDA09	**Data Science and Model Management**	The solution should support data science workflows including data preparation, feature engineering, model development, testing, validation, deployment, version control, model monitoring, retraining, performance assessment, and controlled retirement of analytical and AI models.		
EDA10	**Analytics Platform, Scalability and Performance**	The solution should provide scalable data processing, storage, and analytical capabilities to support enterprise workloads, concurrent users, scheduled and on-demand processing, increasing data volumes, advanced analytics, AI workloads, and high-availability requirements.		
EDA11	**Analytics Security and Access Management**	The solution should support role-based access control, authentication, authorization, data-level security, encryption, segregation of sensitive information, audit trails, usage monitoring, and controlled access to enterprise data, analytical models, datasets, reports, and AI services.		
EDA12	**Analytics Integration and API Services**	The solution should integrate with MSOOS, Power BI, Finance, Procurement, Human Resources, EAM, Billing, SCADA, ATG, Metering, operational systems, external data sources, and other approved enterprise applications through secure REST/SOAP APIs, ETL/ELT pipelines, data interfaces,		

		streaming mechanisms, and other approved integration technologies.		
EDA13	**Analytics Monitoring and Administration**	The solution should support centralized monitoring and administration of data pipelines, integration jobs, data processing, analytical workloads, datasets, dashboards, models, AI services, system performance, failures, usage, and service-level performance, with configurable alerts and escalation.		

2.2.4.2.5.4 Enterprise Monitoring and Response Platforms

Overview

The tenderer shall provide, install, configure, test, and commission an enterprise-grade Enterprise System Monitoring and Response Platform to provide centralized monitoring, observability, event management, performance monitoring, automation, and operational intelligence across the Corporation's Digital Transformation Platform.

The proposed solution shall provide a unified monitoring platform capable of monitoring enterprise infrastructure, applications, databases, networks, cloud services, containers, and operational technology (OT) environments. The platform shall deliver real-time visibility, proactive monitoring, automated response, operational analytics, and enterprise-wide observability to improve service availability, operational resilience, and business continuity.

The Enterprise System Monitoring and Response Platform shall:

i. provide centralized monitoring, observability, and operational visibility across enterprise infrastructure, applications, databases, networks, cloud environments, and operational technology systems;
ii. provide real-time monitoring of infrastructure health, application performance, user experience, service availability, and business-critical operations;
iii. support intelligent event correlation, anomaly detection, predictive analytics, automated incident response, and operational automation;
iv. provide centralized logging, metrics collection, distributed tracing, analytics, reporting, and compliance monitoring;
v. integrate seamlessly with enterprise cybersecurity, IT service management, DevOps, automation, and business continuity platforms;
vi. support scalable, resilient, and highly available monitoring services capable of supporting future business growth;
vii. support automated asset discovery, dependency mapping, root cause analysis, SLA monitoring, and operational reporting; and
viii. provide an OEM-supported Enterprise System Monitoring and Response Platform throughout the contract period.

The proposed solution shall include all software, licences, monitoring components, observability services, analytics capabilities, dashboards, automation services, implementation services, training, and supporting infrastructure required to deliver a fully integrated Enterprise System Monitoring and Response Platform.

Detailed technical requirements are provided in the Enterprise System Monitoring and Response Platform Compliance Matrix below.

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
1.	Provide unified monitoring of infrastructure, applications, databases, containers, and cloud environments through a centralized management console		
2.	Support real-time and near real-time metrics collection, event processing, and alerting with low-latency ingestion pipelines		
3.	Support comprehensive observability including metrics, logs, and distributed tracing with end-to-end correlation capabilities		
4.	Provide AI/ML-driven anomaly detection, predictive analytics, and trend analysis for proactive issue identification		
5.	Support threshold-based, dynamic, and anomaly-based alerting with intelligent correlation and noise reduction mechanisms		
6.	Integrate seamlessly with IT Service Management (ITSM) tools, ticketing systems, and workflow automation platforms		
7.	Support event-driven automation, runbooks, and orchestration through integrations (e.g., Ansible, scripting frameworks)		
8.	Provide automated dependency mapping, topology visualization, and root cause analysis capabilities		
9.	Support application performance monitoring including instrumentation, transaction tracing, end-user monitoring, and synthetic testing		
10.	Support both agent-based and agentless monitoring for operating systems, hypervisors, and hardware devices		
11.	Provide native monitoring of containerized environments including clusters, nodes, pods, and services		
12.	Support comprehensive network monitoring including devices, traffic flows, SNMP, NetFlow, sFlow, latency, and bandwidth utilization		
13.	Provide centralized log management including collection, parsing, indexing, search, and integration with SIEM platforms		
14.	Enforce security controls including role-based access control (RBAC), encryption (in transit and at rest), audit logging, and LDAP/Active Directory integration		
15.	Provide customizable dashboards, KPI tracking, SLA monitoring, and report generation/export capabilities		
16.	Support audit trails and compliance reporting aligned with applicable regulatory and industry standards		

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
17.	Support logical data separation and fine-grained role-based access controls for multi-tenant or segregated environments		
18.	Provide APIs and plugins for integration with CI/CD tools such as Jenkins, GitLab, and Terraform		
19.	Support distributed architecture with clustering, horizontal scalability, and high availability		
20.	Provide high-throughput ingestion pipelines capable of handling large-scale metrics, logs, and tracing data		
21.	Support automated discovery of infrastructure, applications, services, and dependencies		
22.	Provide AI-driven event correlation, deduplication, and alert suppression to improve signal-to-noise ratio		
23.	Enable definition, monitoring, and reporting of SLAs/SLOs with alerts on threshold breaches		
24.	Provide Real User Monitoring (RUM) and synthetic transaction monitoring capabilities		
25.	Support extensibility through plugin frameworks, SDKs, and custom integrations		
26.	Provide backup, replication, and failover mechanisms for the monitoring platform		
27.	Support optimized compute utilization leveraging multi-core CPU architectures for analytics and ingestion workloads		
28.	Support high memory utilization for in-memory processing, correlation, and indexing		
29.	Ensure high availability through redundant components, clustering, and elimination of single points of failure		
30.	Support monitoring of Operational Technology (OT) environments (e.g., SCADA, ICS) with secure integration and strict segregation between IT and OT domains		
31.	Provide configurable incident response workflows, escalation matrices, and collaboration mechanisms for coordinated incident management		
32.	Enable capacity planning, forecasting, and performance optimization using historical and predictive analytics		
33.	Provide business service mapping and service-centric dashboards linking IT performance metrics to business KPIs and operational outcomes		
34.	Support monitoring and reporting of disaster recovery posture, failover readiness, and RTO/RPO compliance		
35.	Provide governance, risk, and compliance dashboards including policy monitoring, risk scoring, and regulatory reporting capabilities		
36.	Provide unified security posture visibility through integration with SIEM, EDR/XDR, and vulnerability management systems		

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
37.	Support monitoring of distributed, remote, and edge environments with capabilities for intermittent connectivity and centralized visibility		

2.2.4.2.6 Mid-Stream Oil Operations Solution

2.2.4.2.6.1 Planning and Scheduling

Overview

The proposed solution shall provide an integrated Planning & Scheduling platform that brings together hydrocarbon supply, demand, importation, inventory, marine, terminal, and pipeline planning within a unified planning environment. It shall support demand forecasting, inventory balancing, replenishment and stock-cover planning, cargo sourcing, vessel and berth scheduling, pipeline nominations and capacity allocation, batch planning and sequencing, resource and throughput optimization, and laytime and demurrage optimization. The solution shall leverage AI, predictive analytics, real-time operational data, constraint-based optimization, and scenario modelling to develop feasible and optimized plans and schedules, considering product availability, tank ullage, infrastructure and pipeline capacity, vessel and terminal constraints, maintenance requirements, contractual obligations, and operational rules. It shall support dynamic replanning in response to changes in demand, inventory, capacity, and operating conditions, while providing planning dashboards, KPIs, analytics, scenario comparison, governance, and traceability to support informed operational and management decision-making.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
OPS01	Hydrocarbon Supply, Demand & Distribution Planning	The solution shall provide integrated, multi-horizon hydrocarbon supply, demand, and distribution planning using statistical and AI-driven forecasting based on historical throughput, customer nominations, seasonal patterns, market trends, and operational data. It shall forecast demand and stock-cover requirements, optimize product allocation, inventory distribution, depot replenishment, vessel requirements, and pipeline movements across terminals, depots, and partner storage facilities, while considering product availability, tank ullage, infrastructure and pipeline capacity, equipment availability, maintenance requirements, contractual commitments, and operational constraints. The solution shall support scenario modelling, what-if analysis, constraint-based and multi-objective optimization, version-controlled planning, and dynamic replanning in response to changes in demand, inventory, supply, capacity, and operating conditions, and provide		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		optimized supply and distribution plans, planning analytics, KPIs, and decision-support dashboards.		
OPS02	Import Planning, Optimization & Replenishment Management	The system shall provide integrated import planning, optimization, and replenishment management that derives import requirements from supply, demand, inventory, and stock-cover plans; optimizes import quantities, timing, sourcing, cargo allocation, vessel nominations, sequencing, and discharge based on terminal capacity, ullage, pipeline throughput, equipment availability, maintenance, and operational constraints; integrates real-time data from SCADA, metering, tankage, run sheet, throughput/sales, and asset management systems; supports stock-cover monitoring, event-driven replanning, scenario/what-if analysis, exception management, alerts, and escalation; incorporates demurrage and detention risks to minimize cost and congestion; and provides import schedules, vessel discharge tracking, KPI analytics, audit trails, and end-to-end visibility of import execution, variances, and supply reliability.		
OPS03	Vessel Scheduling & Berth Management	The system shall provide integrated vessel scheduling, queue management, and berth allocation to optimize vessel sequencing and terminal utilization based on berth capacity, vessel compatibility, cargo requirements, ullage, discharge capacity, and scheduling constraints; identify and resolve berth conflicts; support planned laytime and demurrage/dispatch estimation; enable scenario modelling of alternative vessel and berth schedules; and provide optimized vessel arrival, berth allocation, and discharge schedules.		
OPS04	Pipeline Nominations & Scheduling	The system shall provide integrated pipeline nomination, capacity allocation, scheduling, sequencing, and pumping plan optimization based on shipper requirements, contractual entitlements, demand, infrastructure capacity, and operational constraints; monitor and reconcile planned versus actual pipeline movements and throughput; and provide alerts and exception management for disruptions, capacity breaches, scheduling conflicts, and throughput variances.		
OPS05	Pipeline Batch Planning & Interface/Transmix Forecasting	The system shall provide optimized pipeline batch planning and interface forecasting based on demand, inventory, terminal constraints, and operational data; define batch structures,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		sequencing, routing, sizing, and movement timelines; forecast product interfaces to minimize losses and improve pipeline utilization; support scenario analysis and exception identification; align batch plans with vessel, terminal, and downstream requirements; and generate schedules, interface forecasts, utilization plans, and execution-ready outputs.		
OPS06	Integrated Planning & Optimization Engine	The system shall provide a centralized planning and optimization engine integrating demand, supply, imports, vessels, pipelines, and batch plans into synchronized end-to-end execution plans; use real-time inventory and operational feedback to support dynamic, exception-driven replanning; incorporate commercial and operational constraints; provide multi-objective optimization, scenario analysis, dependency management, performance analytics, and comprehensive auditability of planning decisions and overrides.		
OPS07	Ullage Creation Schedule & Optimized Batch Sequencing	The system shall provide dynamic ullage-driven batch and pumping optimization using real-time stock, ullage, demand, receipts, capacity, and operational constraints; optimize batch sizing, sequencing, timing, and pipeline utilization with end-to-end batch traceability; coordinate vessel, berth, discharge, and pipeline schedules; incorporate AI-driven optimization and maintenance constraints; support alerts, dynamic replanning, and disruption scenarios; and provide dashboards for batch execution, vessel containment, schedules, and planned-versus-actual performance.		
OPS08	Global Stock Projection & Import Optimization	The system shall provide enterprise-wide stock projection and import optimization by maintaining real-time visibility of pumpable stock, ownership, location, reserves, blocked stock, and other inventory constraints; forecast demand and stock-cover days; optimize cargo nominations, imports, replenishment, and delivery schedules based on projected demand, ullage, capacity, and operational constraints; support AI forecasting, scenario analysis, demurrage and disruption modelling; and provide inventory risk dashboards, reporting, and integration with Tankage, Run Sheet, Throughput/Sales, and Asset Management systems.		
OPS09	Mainline Scheduling &	The system shall provide AI-driven mainline scheduling and pipeline optimization covering		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Pipeline Optimization	batch sequencing, pumping cycles, flow rates, transit times, interfaces, and delivery schedules based on demand, stock, ullage, capacity, product priorities, and operational rules; synchronize plans with real-time execution, Tankage, SCADA, metering, Run Sheet, Throughput/Sales, and Asset Management systems; optimize utilization while minimizing interfaces and operational risks; support disruption-driven replanning, exception management, reconciliation, KPI analytics, and complete audit trails.		
OPS10	Terminal Replenishment Planning & Optimization	The system shall provide terminal-level replenishment planning and optimization using opening stock, demand forecasts, service levels, pipeline capacity, flow rates, ullage, containment, and operational constraints to determine replenishment quantities, frequency, batch sizes, and sequencing; dynamically adjust plans using real-time execution and demand data; incorporate maintenance and pipeline constraints; integrate Tankage, SCADA, metering, Run Sheet, and Throughput/Sales systems; and provide replenishment schedules, batch tracking, stock-cover monitoring, and exception dashboards.		
OPS11	Pipeline Capacity Allocation Management	The system shall provide automated, transparent, and rules-based pipeline capacity allocation to eligible OMCs, considering available capacity, ullage, regulatory and financial eligibility, contractual and operational determinants, and infrastructure constraints; integrate with regulatory, financial, Tankage, Stock, and Throughput systems for continuous validation; provide secure OMC self-service nomination, documentation, allocation tracking, notifications, and lifecycle management; support revisions, version control, auditability, exception handling, and allocation variance analysis; and provide capacity, special allocation, missed allocation, and utilization dashboards.		
OPS12	Partner Country Allocation, Drawdown & Inventory Planning	The system shall provide Partner Country allocation, drawdown, and inventory planning capabilities to maintain visibility of stock positions by country, product, ownership, and location; calculate and optimize allocations, entitlements, replenishment requirements, and projected drawdowns based on approved nominations and supply plans; support end-to-end batch and stock traceability across marine receipts, storage,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		pipeline movements, and depot uplifts; integrate with inventory, vessel, berth, and operational systems; and provide allocation scenarios, stock projections, exception alerts, dashboards, KPIs, and audit trails to support transparent and optimized Partner Country stock management.		
OPS13	Demurrage Planning, Simulation & Optimization	The system shall support demurrage exposure modelling and optimization by incorporating contractual laytime terms, vessel schedules, berth availability, cargo readiness, discharge windows, terminal capacity, tank ullage, pipeline availability, and pumping constraints into planning decisions; enable scenario and what-if analysis of alternative vessel, berth, discharge, and pipeline schedules; forecast potential demurrage exposure and identify key cost drivers; and provide optimized scheduling recommendations, alerts, KPIs, and planning analytics to minimize demurrage costs and vessel delays.		
OPS14	Resource, Capacity & Throughput Planning	The solution shall support integrated planning and optimization of pipelines, terminals, tanks, pumps, loading bays, berths, equipment, and other operational resources, considering capacity, ullage, product availability, maintenance, flow constraints, and operational dependencies. It shall identify bottlenecks and resource conflicts, optimize capacity utilization and throughput, support scenario and what-if analysis, and provide capacity forecasts, resource requirements, throughput projections, and planning KPIs.		
OPS15	Planning Version, Baseline & Scenario Management	The system shall provide controlled planning version and scenario management, enabling users to create, save, compare, approve, revise, and retrieve planning versions and scenarios, with clear identification of assumptions, changes, approvals, overrides, and effective dates to ensure traceability and governance of planning decisions.		
OPS16	Planning Analytics, KPIs & Decision Support	The system shall provide integrated planning analytics and decision-support dashboards covering demand forecasts, inventory and stock-cover projections, supply and replenishment plans, import and vessel schedules, pipeline capacity and utilization, batch plans, resource utilization, planning scenarios, forecast variance, schedule performance, and optimization outcomes, with configurable KPIs, trend analysis, scenario comparison, and audit-traceable planning information.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
OPS17	Planning Integration & Governance	The solution shall integrate with relevant enterprise and operational systems, including Marine Operations, Terminal Management, Inventory Management, Order Management, Maintenance and Enterprise Asset Management, SCADA, GIS, Financial Management, and Analytics platforms, to provide the data required for integrated planning and scheduling. It shall support role-based access, configurable workflows, approvals, notifications, version control, audit trails, and traceability of planning decisions, assumptions, overrides, and schedule revisions.		

2.2.4.2.6.2 Marine Operations

Overview

The proposed solution shall provide an integrated Marine Operations capability to support the execution, coordination, monitoring, reconciliation, and control of petroleum marine receipt, discharge, backloading, and transfer operations. The solution shall provide real-time operational visibility, safety and quality controls, quantity and custody reconciliation, inventory and entitlement updates, demurrage verification, regulatory compliance, exception management, and integration with relevant enterprise and external systems to ensure safe, efficient, reliable, compliant, and auditable marine operations.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MO03	Marine Receipt, Discharge & Transfer Operations	The solution shall support end-to-end marine nomination, receipt, discharge and transfer workflows, including nomination capture and validation, cargo receipt planning, berth scheduling coordination, cargo manifest validation, tank allocation, vessel/shore cargo validation, discharge-plan validation, operational approvals, discharge execution, quantity determination, custody and title transfer, reconciliation, outturn confirmation and posting, transaction closure, and configurable workflows, approval hierarchies and operational rules across multiple terminals and ports.		
MO04	Vessel, Berth & Resource Coordination	The solution shall support operational coordination of vessels, berths, pilots, tugs, inspectors, surveyors, contractors, equipment and other marine resources in accordance with approved schedules and operational plans, including vessel and berth readiness, Notice of Readiness (NOR) generation, issuance and tracking, operational handover, connection/disconnection readiness, turnaround monitoring, and coordination of marine stakeholders.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MO05	Marine Monitoring, Measurement & Reconciliation	The solution shall provide real-time monitoring and capture of marine operational events and measurements through integration with SCADA, terminal automation, metering, ATG, surveyor systems and other operational sources, including flow rates, pressures, temperatures, tank levels, start/stop events, stoppages, transferred quantities, vessel/shore figures, tank dipping and Tank Dipping Reports (TDR), and surveyor measurements. The solution shall support controlled tank-switching workflows, including receiving-tank validation, ullage verification, product compatibility and alignment with approved discharge plans. It shall reconcile nominated, contracted, metered, vessel, shore, TDR, surveyor and operational quantities using approved temperature, density, metering correction and standard-volume conversion methodologies in accordance with applicable API, ASTM and regulatory requirements, identify variances, support investigation and approval, and enable validated outturn reconciliation and posting.		
MO06	Marine Safety, Quality & Operational Control	The solution shall support marine safety and operational controls including Permit-to-Work, pre-discharge meetings, safety confirmations, inspections, vessel and cargo readiness verification, loading/discharge authorization, loading arm connection and disconnection approvals, emergency shutdown, operational suspension and recovery, sampling, laboratory testing, quality acceptance, configurable settling, draining, sampling, inspection and release workflows, quarantine, rejection and cargo/tank release. The solution shall support automated quality-based acceptance, quarantine or rejection decisions and generation and approval of applicable Tank Release Certificates and quality clearance documentation.		
MO07	Cargo, Ownership & Entitlement Management	The solution shall support multi-customer and multi-owner cargo management, including cargo allocation, split ownership, quantity assignment, ownership tracking, entitlement validation, configurable custody and title transfer points, effective transfer timestamps, validated transfer quantities and reconciliation approvals, and real-time updating of inventory and customer entitlement positions following approved marine transactions.		
MO08	Backloading / Ship Re-Loading Operations	The solution shall support controlled execution of approved backloading operations, including request validation, vessel and cargo readiness, stock and entitlement validation, cargo compatibility, tank and berth readiness, loading authorization, real-time loading monitoring, quantity reconciliation, inventory and entitlement updates, marine documentation, and operational closure.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MO09	Marine Documentation, Compliance & Governance	The solution shall support generation, approval, distribution, storage, retrieval, version control, and archival of Bills of Lading, cargo manifests, survey reports, certificates, permits, reconciliation statements, voyage records, and regulatory submissions. The solution shall provide configurable workflows, maker-checker controls, delegated authority, segregation of duties, role-based access, notifications, escalations, SLA monitoring, comprehensive audit trails, and integration with applicable customs, port, tax, maritime, and regulatory platforms.		
MO10	Marine Exception, Risk & Incident Management	The solution shall support identification, recording, escalation, investigation, and resolution of marine exceptions, risks, incidents, delays, quantity variances, quality failures, berth conflicts, transfer interruptions, metering discrepancies, leaks, abnormal pressure/flow conditions, equipment failures, emergency events, and other non-conformances, including root-cause analysis and corrective-action tracking.		
MO11	Demurrage, Performance & Marine Analytics	The solution shall capture actual vessel operational events including NOR, berthing, all-fast, discharge commencement/completion, stoppages, stripping, and departure; calculate and verify contractual laytime and demurrage exposure; reconcile discharged quantities; support demurrage simulation and root-cause analysis; identify delay and cost drivers; and provide dashboards, reports, KPIs, alerts, benchmarking, and trend analysis covering vessel turnaround, berth utilization, discharge performance, pumping efficiency, laytime compliance, operational losses, demurrage exposure, recurring bottlenecks, and demurrage reduction initiatives.		
MO12	Marine Systems Integration & Transaction Synchronization	The solution shall integrate with Planning & Scheduling, Vessel and Berth Management, Terminal Operations, Tankage, Inventory and Stock Management, Customer Entitlement, Quality/Laboratory, SCADA, ATG, metering, Demurrage, Billing, Financial Management, Enterprise Asset Management, Enterprise Document & Records Management, port and regulatory systems, and other relevant enterprise or external systems to synchronize operational events, measurements, inventory, entitlement, commercial, financial, regulatory, and reporting data.		
MO13	Surveyor Reconciliation & External Submission Portal	The solution shall provide a secure portal or controlled digital interface for authorized surveyors to submit, review and track vessel figures, shore figures, TDRs, outturn reports, discrepancy reports, supporting documentation and reconciliation records. The solution shall support configurable maker-checker controls, validation, approval, rejection, amendment, escalation and status tracking of surveyor submissions, with		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		complete audit trails and controlled integration into marine reconciliation and outturn processes.		

2.2.4.2.6.3 Pipeline Operations & Transportation

Overview

The proposed solution shall provide an integrated Pipeline Operations & Transportation capability to support the safe, reliable, efficient, and auditable execution of petroleum movements across the pipeline network, providing real-time visibility of pipeline and batch movements, transfer and replenishment operations, pipeline performance and integrity, measurement, reconciliation, custody transfer, and inventory updates through integration with SCADA, metering, tankage, stock management, planning, terminal, and external systems. The solution shall support operational decision-making through pipeline optimization, interface and loss management, DRA and corrosion inhibitor management, PIG operations, exception management, performance analytics, and controlled operational workflows, while maintaining end-to-end traceability and ensuring that control and physical actuation remain within the appropriate SCADA/industrial control systems.

Functional Requirements

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
POT01	Pipeline Batch Execution Monitoring & Reconciliation	The system shall provide real-time visibility and traceability of pipeline batch movements using SCADA and metering data, maintaining unique batch identifiers and standardized lifecycle states from planned release through receipt and reconciliation. It shall track batch splits, merges, interfaces, re-routing, stoppages, and operational adjustments; perform planned-versus-actual reconciliation, interface accounting, gain/loss analysis, and exception management; and provide alerts, audit trails, KPIs, historical trends, and operational analytics. Integration shall be provided with Planning, Tankage, Stock Management, Batch Management, SCADA, and Mainline Metering systems.		
POT02	Mainline Transfer to Partner Terminals	The system shall support end-to-end management of pipeline transfers to partner terminals, including secure customer/partner requests, entitlement and operational validation, approvals, scheduling, batch sequencing, execution monitoring, custody transfer and ownership, reconciliation, inventory updating, and closure. It shall validate product availability, tank/ullage capacity, pipeline and terminal readiness, capacity, operational and regulatory constraints, capture tank, ATG, metering and SCADA measurements, support automated start/mid/end-		

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
		batch sampling and LIMS workflows, apply standardized quantity conversion and reconciliation, and update source and receiving inventory following validated transfer. The solution shall maintain configurable transfer lifecycle states, manage exceptions and escalations, provide notifications, audit trails, operational dashboards and reconciliation reporting, and integrate with SCADA, metering, Tankage, Stock Management, Batch Management, LIMS, partner-terminal and regulatory systems, including partner-terminal performance analytics.		
POT03	Mainline Receipt from Partner Terminals	The system shall support end-to-end management of mainline receipts from partner terminals, including customer nomination, validation, approval, batch planning, pipeline capacity reservation, scheduling, and integration with supply planning. It shall provide real-time execution monitoring and lifecycle tracking, capture SCADA and metering data for custody transfer and quantity standardization, validate tankage, pipeline, vessel, terminal, product, batch, contractual and regulatory constraints, and update inventory following validated receipt. The solution shall support exception management, notifications, reconciliation, audit trails, regulatory and stakeholder integration, and operational analytics, including vessel performance and demurrage insights.		
POT04	Line Transfers to Depots	The system shall support operational monitoring and execution of depot replenishment transfers based on approved plans and schedules, including visibility of stock levels, transfer priorities, batch movements, and execution status. It shall monitor tankage, pipeline, and operational constraints; track transfers using SCADA and metering data; manage product interfaces, interruptions, and execution variances; reconcile planned/approved quantities against actual movements; and provide alerts, exception management, audit trails, and operational performance dashboards. The system shall integrate with Planning & Scheduling, Tankage, Stock Management, SCADA, Mainline Metering, and Enterprise Asset Management systems to receive approved transfer requirements and relevant operational data.		
POT05	Pipeline Optimization & DRA Management	The system shall provide decision-support for optimizing pipeline throughput, hydraulic performance, energy efficiency, batch sequencing, flow rates, and DRA utilization. It shall use SCADA, metering, stock, tankage,		

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
		batch, and asset data to analyse current and historical performance, estimate DRA requirements, evaluate alternative operating scenarios, identify hydraulic constraints and inefficiencies, and recommend optimized operating strategies. It shall track planned versus actual DRA usage, provide configurable optimization rules and alerts, and deliver KPI, trend, benchmarking, and optimization analytics with full auditability.		
POT06	Line Cleaning / Pipeline Inspection Gauging (PIG) Operations	The system shall support controlled PIG operations through configurable workflows, readiness and safety validation, PTW approvals, capacity coordination, and operational monitoring. It shall maintain a PIG asset register, track launch, travel, and retrieval events, receive SCADA and tracking information, identify abnormal conditions such as stuck pigs, pressure deviations, delays, and blockage risks, and support emergency and recovery workflows. The system shall provide post-operation validation, performance analytics, reporting, and complete audit trails while PIG actuation remains under the relevant operational control systems.		
POT07	Pipeline Integrity Management Integration	The system shall integrate with Pipeline Integrity Management, SCADA, In-Line Inspection and Pigging (ILI/PIG), GIS, maintenance, Risk-Based Inspection (RBI), cathodic protection, and leak detection systems to consolidate pipeline integrity information and provide operational visibility. It shall monitor integrity risks and operational constraints, provide configurable thresholds and alerts, support defect and mitigation workflows, and provide predictive analytics for degradation, remaining useful life, and risk trends. It shall provide integrity dashboards, risk analysis, inspection and compliance reporting, and complete traceability of integrity-related decisions and constraints.		
POT08	Corrosion Inhibitor Dosing Management	The system shall monitor corrosion inhibitor availability and dosing performance using SCADA inputs, maintain inhibitor inventory and depletion projections, and provide configurable alerts and replenishment workflows. It shall validate dosing readiness, manage approved dosing rates and product/line selection rules, initiate and terminate dosing workflows based on operational movement windows, monitor actual injection against approved parameters, and manage deviations, equipment failures, communication issues, corrective actions, and reconciliation. Physical pump and valve actuation		

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
		shall remain under SCADA control, with all dosing activities, approvals, QC inputs, and execution data fully auditable.		
POT09	Tank Decommissioning & Commissioning Management	The system shall support controlled decommissioning and commissioning of tanks through workflow-based approvals, operational dependency assessment, tank availability management, and continuity-of-supply planning. It shall recommend suitable alternative tanks based on ullage, compatibility, and operational constraints; integrate with SCADA and measurement systems for monitoring and quantity reconciliation; manage tank dipping and Tank Dipping Report(TDR) processes; prevent use of decommissioned tanks until formally reactivated; and support commissioning checklists, safety and integrity validation, baseline/zero-balance verification, ERP alignment, associated pipeline commissioning, and complete audit trails.		
POT10	Jet A-1 Handling Management	The system shall provide controlled end-to-end Jet A-1 receipt and handling, including schedule ingestion, tank compatibility and ullage validation, QC clearance, pre-receipt measurements, valve-lineup readiness, contamination prevention, and real-time SCADA/metering monitoring. It shall manage in-process and UML sampling, laboratory workflows, settling periods, final measurements, standardized quantity reconciliation, inventory and entitlement updates, exception handling, and generation of TDRs, QC certificates, and receipt reports. All activities and measurements shall be fully traceable and auditable.		
POT11	Pipeline Packing Delivery – Multi-Purpose Line (MPL)	The system shall support controlled MPL delivery transactions by capturing and validating tank dips, ATG readings, custody-meter outputs, stock positions, QC results, and SCADA operational data. It shall enforce readiness and approval workflows, custody-transfer rules, standardized quantity conversion, meter/ATG/dip reconciliation, exception management, and post-closure certification. Validated quantities shall update stock positions, with delivery, reconciliation, variance, exception, and regulatory reports generated against a unique MPL transaction reference and supported by a tamper-evident audit trail.		
POT12	Line Lease Transfer Process	The system shall provide secure self-service and workflow-based management of line lease transfers from request initiation through approval, execution, reconciliation, billing, regulatory submission, and closure, with unique transaction		

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
		references and real-time lifecycle visibility. It shall support OMC and authorized internal requests, document submission and generation, role segregation and maker-checker controls, defined lifecycle states, custody and ownership rules, standardized quantity and valuation methods, and reconciliation of approved quantities, operational execution, inventory, and financial postings. The solution shall manage exceptions, reversals, failed postings and integration failures through controlled workflows, trigger automated billing and revenue processing based on approved tariffs and contractual terms, integrate with financial and regulatory systems including KRA, and provide configurable notifications, escalation alerts, comprehensive operational and financial reporting, transfer and billing documentation, and tamper-evident audit trails.		
POT13	Batch Letters Management	The system shall manage the complete lifecycle of batch-related declarations and communications, including Notice of Intention capture and validation, batch receipt confirmation, FIFO-based allocation and proration, configurable letter templates, automated document generation, digital signatures, distribution, tracking, acknowledgment, reconciliation, and exception management. It shall maintain version-controlled records, historical correspondence, approvals, allocation results, and audit trails and provide reporting for operational, regulatory, and customer requirements.		

2.2.4.2.6.4 Oil Stocks & Inventory Management

Overview

The proposed solution shall provide an integrated enterprise-wide Oil Stocks & Inventory Management capability for real-time management of petroleum inventory across receipts, storage, transfers, custody transfer, dispatch, blending, adjustments, and other stock movements. It shall manage physical and book stock through a centralized Banking/Grid Logistics Model with virtual depot–tank structures, customer ownership and entitlements, trading and linefill stock, inventory reconciliation, gain/loss, stock controls, customer self-service, stock statements, and linefill management. The centralized ledger shall serve as the authoritative source for operational, commercial, financial, entitlement, and regulatory inventory positions, with secure integration across relevant operational, enterprise, customer, and regulatory systems.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
INV01	Central Inventory Ledger and Product Fungibility	The solution shall maintain a centralized inventory ledger based on a Banking/Grid Logistics Model, using a standardized virtual depot–tank structure to provide an enterprise-wide view of customer-owned hydrocarbon stocks independently of physical storage location. The ledger shall serve as the authoritative source for operational, commercial, financial, entitlement, and regulatory inventory positions.		
INV02	Trading, Linefill & Inventory Categories	The solution shall support configurable virtual inventory categories, including at minimum Trading Tank and Linefill Tank, with rules governing commercial availability, operational use, ownership, transfers, contributions, withdrawals, and replenishment. Linefill stock shall remain non-tradable unless explicitly authorized under defined business rules.		
INV03	Customer Ownership & Entitlement	The solution shall maintain customer-owned inventory and entitlement positions within the centralized ledger, including product, customer, duty status, financing status, quality status, allocation, quotas, contractual obligations, credit limits, product eligibility, and other applicable business rules. It shall support global utilization of customer entitlements across integrated locations subject to operational and governance controls.		
INV04	Stock Availability, Financing & Collateral Financing Agreement (CFA) Controls	The solution shall determine stock availability and transaction eligibility based on customer entitlement, product and quality status, regulatory restrictions, operational readiness, financing/CFA status, and other configurable controls. Financed or collateralized stock shall remain restricted from allocation, transfer, or delivery until formally released through an approved governance process.		
INV05	Tank & Physical Stock Management	The solution shall provide real-time visibility of physical tank stock, capacity, available stock, ullage, dead stock, operational reserves, product segregation, and utilization using integrated ATG, SCADA, metering, and approved manual measurement inputs (Dip tickets).		
INV06	Measurement, Calibration & Quantity Conversion	The solution shall support controlled management and validation of tank dips, calibration and strapping tables, temperature and density corrections, quantity conversion, measurement tolerances, and maker-checker approvals to ensure accurate and consistent inventory quantities.		
INV07	Inventory Reconciliation & Variance Management	The solution shall reconcile physical and book stock using tank measurements, ATG, SCADA, metering, operational transactions, pipeline movements, surveyor data, and other approved sources. It shall identify, investigate, classify,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		approve, and resolve variances through controlled workflows and configurable tolerances.		
INV08	Gain & Loss Management	The solution shall calculate, allocate, reconcile, and report gains and losses at tank, facility, terminal, depot, pipeline, customer, product, logistics-mode, and enterprise levels using configurable methodologies, tolerances, and approval controls, with approved results reflected in inventory and entitlement balances.		
INV09	Linefill Management	The solution shall support customer linefill contribution, withdrawal, temporary withdrawal, eligibility and threshold checks, supporting-document validation, multi-level maker-checker approvals, entitlement updates, replenishment-period tracking, reconciliation against operational and Outturn data, automatic reinstatement of temporary withdrawals upon replenishment, exception handling, notifications, and complete auditability.		
INV10	Inventory Status & Quality Controls	The solution shall support configurable inventory states including unrestricted, quality inspection, released, quarantined, off-specification, restricted, financed, and blocked stock, with controls preventing unauthorized allocation, transfer, or dispatch of ineligible product.		
INV11	Inventory Movement & Custody Transfer	The solution shall integrate and track marine receipts, pipeline transfers, inter-terminal and tank-to-tank transfers, truck and rail dispatches, hydrant deliveries, MPL operations, blending, and other logistics events, ensuring ownership, entitlement, availability, and ledger postings are updated only upon validated operational and custody-transfer events.		
INV12	Marine Receipt & Outturn Reconciliation	The solution shall support provisional recording and subsequent validation of marine receipts using quality clearance, custody-transfer measurements, surveyor/outturn reports, linefill declarations, and reconciliation controls before stock and entitlement are released for commercial use.		
INV13	Inventory & Exchanges	The solution shall provide controlled workflows for inventory and Adjustment of Stock Entitlement (ASE) transactions, including initiation, validation, document verification, maker-checker approval, CFA/financing validation, rejection, execution, reversal, exception handling, escalation, and synchronization with the central inventory ledger while preserving the original transaction history.		
INV14	Customer Self-Service & Entitlement Access	The solution shall provide secure, role-based customer self-service access to inventory and entitlement positions, account statements, receipts, deliveries, journal vouchers, entitlement		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		adjustments, linefill positions, supporting documents, and service requests. Customers shall be able to initiate and track authorized entitlement and linefill requests with real-time status visibility.		
INV15	Customer Stock Statements	The solution shall generate customer stock statements from the centralized inventory ledger, supporting configurable content, dimensions, templates, reporting periods, cut-off rules, scheduled, event-driven and on-demand generation, and presentation of opening balances, receipts, transfers, deliveries, entitlement movements, gain/loss allocations, adjustments, linefill movements, and closing balances. Statements shall support validation, reconciliation, maker-checker approval, digital signing, multi-channel distribution, customer self-service access, transaction drill-down, controlled reprocessing, version control, archival, and retention.		
INV16	Inventory, Entitlement & Linefill Exceptions	The solution shall provide structured exception and discrepancy management covering inventory variances, entitlement adjustments, ASE failures, linefill discrepancies, incomplete replenishments, failed postings, conflicting transactions, and integration failures, with investigation, classification, escalation, resolution, approval, and audit-controlled correction.		
INV17	Inventory Governance, Security & Auditability	The solution shall provide role-based access, segregation of duties, maker-checker and multi-level approvals, transaction authorization, notifications, and tamper-evident audit trails covering measurements, movements, postings, reconciliations, entitlement changes, ASE transactions, linefill transactions, statement processing, calibration changes, overrides, reversals, and adjustments. Completed ledger postings and approved statements shall be protected from unauthorized alteration or deletion.		
INV18	Inventory Master Data & Business Rules	The solution shall support governed management of products, tanks, facilities, capacities, measurement parameters, customers, ownership, inventory categories, quality status, entitlements, financing/CFA status, linefill rules, contractual limits, thresholds, and transaction eligibility rules.		
INV19	Integration & Single Source of Truth	The solution shall integrate with SCADA, ATG, custody-transfer metering, TAS, terminal automation, LIMS/laboratory, pipeline, marine/vessel, planning and scheduling, order management, customer portal, ERP, billing, financial, regulatory, surveyor, document management, and reporting systems. The centralized inventory ledger shall serve as the authoritative source for inventory, entitlement,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		linefill, reconciliation, gain/loss, and related operational, commercial, and financial reporting.		
INV20	Reporting, Analytics & Regulatory Reporting	The solution shall provide configurable dashboards and reports covering stock positions, customer balances, entitlements, utilization, tank capacity and ullage, linefill, inventory ageing and turnover, gains/losses, variances, reconciliation status, stock movements, ASE activity, customer statements, and operational KPIs, with drill-down and export capabilities. It shall support regulatory, statutory, customer, operational, and management reporting and electronic submission where required.		
INV21	Documents, Notifications & Records Management	The solution shall support secure upload, validation, generation, distribution, retrieval, versioning, archival, and retention of inventory and entitlement documents, including receipts, deliveries, JVs, ASE records, Outturn reports, Bills of Lading, linefill documentation, stock statements, reconciliation records, and supporting evidence. It shall provide configurable notifications and alerts for approvals, adjustments, linefill events, statement processing, exceptions, failures, and other material inventory events.		

2.2.4.2.6.5 Order-to-Cash & Product Delivery Management

Overview

The solution shall provide an integrated Order-to-Cash (O2C) and Product Delivery capability covering customer orders, nominations, entitlements, allocations, credit and commercial validation, delivery scheduling and execution, product loading and transfer, custody transfer, quantity capture and reconciliation, delivery documentation, inventory and entitlement updates, billing triggers, invoicing, exceptions, and integration with inventory, terminal, logistics, ERP, finance, and regulatory systems. The solution shall provide complete visibility and traceability from customer order through product delivery, settlement, and closure.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
O2C01	Customer, Product & Commercial Master Data	The solution shall provide governed management of customer, product, facility, contract, pricing, tariff, credit, entitlement, vehicle, vessel, aircraft and other commercial/operational master data, including KYC, validity controls, document management, versioning, maker-checker and audit trails.		
O2C02	Order-to-Cash & Commercial Order Management	The solution shall provide an integrated Order-to-Cash (O2C) and Product Delivery capability covering customer orders, nominations, entitlements, allocations, credit and commercial validation, delivery scheduling and execution, product loading and transfer, custody transfer, quantity capture and reconciliation, delivery documentation, inventory and		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		entitlement updates, billing, invoicing and settlement, exception and dispute management, and integration with inventory, terminal, logistics, ERP, finance and regulatory systems. The solution shall provide complete end-to-end visibility and traceability from customer demand and order creation through product fulfilment, delivery, inventory and entitlement update, billing, settlement and closure.		
O2C03	Product Delivery & Fulfilment Management	The solution shall provide a common end-to-end product fulfilment and delivery orchestration capability for approved petroleum product orders across applicable delivery modes, including pipeline/pump-over, marine backloading, truck and wagon loading, hydrant delivery and other authorized delivery channels. It shall support delivery scheduling, resource allocation, execution coordination, quality clearance, custody-transfer and quantity capture, delivery confirmation, inventory and entitlement updates, reconciliation, exception management and closure, while integrating with the specialized operational systems supporting each delivery mode.		
O2C04	Pump-over Delivery Management	The solution shall support controlled end-to-end pump-over delivery, including request capture, entitlement and stock validation, product quality and tank compatibility checks, ullage verification, operational readiness, approval and release, SCADA/ATG/metering integration, quantity determination and conversion, reconciliation, inventory posting, exception management, regulatory reporting and complete auditability. The solution shall consume SCADA operational data for monitoring and validation and shall not issue direct process-control commands.		
O2C05	Marine Backloading Management	The solution shall support end-to-end shore-to-vessel backloading, including vessel and cargo validation, entitlement and stock checks, berth and tank readiness, marine approvals, pre- and post-transfer measurements, SCADA/metering integration, loading monitoring, quantity determination, custody-transfer reconciliation, Bill of Lading and cargo documentation, inventory and entitlement updates, regulatory submissions, exception handling and audit trails.		
O2C06	Truck & Wagon Loading Management	The solution shall support end-to-end truck and wagon loading, including order validation, entitlement and product checks, vehicle and driver verification, loading authorization, scheduling, bay allocation, quality clearance, FAN/BOL generation, TAS/AccuLoad version 3/4 integration, loading execution and quantity capture, reconciliation, inventory and entitlement posting, gate release,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		regulatory integration, exception handling, operational reporting and complete auditability.		
O2C07	Hydrant Fuel Delivery Management	The solution shall support end-to-end hydrant fuel delivery, including customer and aircraft request capture, entitlement and stock validation, scheduling, authorization, integration with Hydrant Management Systems, receipt of delivered quantities and transaction status, inventory and entitlement updates, quantity conversion, reconciliation, delivery confirmation, billing triggers, exception management, regulatory reporting and complete transaction traceability.		
O2C08	Delivery Documentation, Billing & Settlement	The solution shall support generation and controlled management of delivery notes, proof of delivery, Bills of Lading, Filling Advice Notes, quality certificates, shipment confirmations and other applicable documentation, and shall trigger billing, invoicing and related financial postings based on validated and reconciled delivery quantities, applicable pricing, contractual terms and approved commercial transactions, with integration to ERP, accounts receivable and financial management systems.		
O2C09	Reconciliation, Exceptions & Dispute Management	The solution shall provide end-to-end reconciliation between orders, nominations, planned quantities, operational measurements, custody-transfer quantities, inventory, customer entitlements and billing records. It shall support configurable tolerances, variance analysis, investigation, adjustment approvals, partial or failed deliveries, integration failures, customer disputes, claims, escalation and resolution workflows, with complete audit trails.		
O2C10	O2C & Delivery Reporting and Analytics	The solution shall provide real-time dashboards and reporting across the O2C and product delivery lifecycle, including order status, fulfilment performance, delivery volumes, customer entitlement utilization, inventory impacts, reconciliation status, billing status, exceptions, truck turnaround, terminal throughput, service levels and commercial KPIs, with drill-down and audit traceability.		

2.2.4.2.6.6 Collateral Finance & Financed Inventory Management

Overview

The proposed solution shall provide an integrated Collateral Finance & Financed Inventory Management capability to manage collateral finance agreements, financing facilities, financier relationships, collateral conditions, financed petroleum stocks, and product-release controls throughout their lifecycle. The solution shall integrate with the centralized Banking/Grid Logistics inventory ledger and virtual depot–tank model to ring-fence financed stock, enforce financing restrictions, process authorized releases to trading inventory, maintain accurate customer entitlements and financing exposure, and provide complete traceability across commercial, operational, financial, and regulatory processes.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CFA01	Collateral Finance Agreement & Facility Management	The solution shall support end-to-end lifecycle management of tripartite collateral finance agreements between KPC, customers, and financing institutions, including stakeholder onboarding, agreement creation, authoring, review, approval, execution, amendment, renewal, suspension, termination, and closure. It shall manage participating financiers, financing facilities, limits, validity periods, approved customers and products, collateral instruments, contractual conditions, and supporting documentation.		
CFA02	Financing & Collateral Validation	The solution shall validate customer eligibility, agreement validity, available financing limits, facility utilization, collateral status and coverage, approved products, contractual conditions, and applicable financing controls before authorizing relevant petroleum orders, allocations, loading, transfers, or deliveries.		
CFA03	Financed Inventory & Banking Ledger Integration	The solution shall integrate with the centralized Banking/Grid Logistics inventory ledger and virtual depot–tank model to identify, allocate, ring-fence, and track financed stock by customer, financier, product, financing facility, cargo, and location. It shall ensure that financing status, inventory availability, and customer entitlement positions remain synchronized with the authoritative inventory ledger.		
CFA04	Financed Stock Blocking, Entitlement & Release Management	The solution shall enforce controlled blocking, restriction, allocation, transfer, and release of financed inventory. CFA-restricted stock shall not be available for unauthorized trading, allocation, loading, transfer, or delivery. Authorized releases shall transfer the applicable quantity from financed/blocked inventory to available trading inventory and automatically update financing positions, inventory balances, and customer entitlements in accordance with approved business rules.		
CFA05	Financing Authorization, Notifications & Workflow Management	The solution shall support automated receipt, validation, and processing of financing notifications, confirmations, bank approvals, release instructions, and related communications. It shall provide configurable workflows for stock blocking, release authorization, exceptions, and approvals, including role-based authorization, maker-checker controls, segregation of duties, delegated authority, escalation, notifications, and complete audit trails.		
CFA06	Facility Utilization, Exposure &	The solution shall provide real-time monitoring of financing limits, utilized and available facilities,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Compliance Monitoring	financed and released stock, outstanding exposure, collateral coverage, expiry dates, contractual obligations, and applicable compliance conditions. It shall provide configurable thresholds, alerts, notifications, and escalation workflows for approaching or breached limits, expiries, pending actions, and other critical CFA events.		
CFA07	CFA Documentation & Collaboration	The solution shall provide secure CFA collaboration and document management capabilities for KPC, customers, and financing institutions, including agreement templates, agreements, amendments, side letters, Pre-Third-Party Holding Certificates (PRE-TPHCs) and other certificates, guarantees, insurance documents, bank confirmations, collateral records, and related correspondence. It shall support controlled document exchange, review, approval, versioning, retention, retrieval, electronic approvals, and digital signatures where applicable.		
CFA08	Reconciliation & Exception Management	The solution shall reconcile financing positions, collateral coverage, financed inventory, stock releases, customer entitlements, and inventory ledger balances using configurable rules and tolerances. It shall support investigation, adjustment, approval, and resolution of discrepancies, expired facilities, limit breaches, unauthorized releases, entitlement mismatches, and other CFA exceptions.		
CFA09	Banking & Enterprise Integration	The solution shall integrate through secure APIs or other approved interfaces with banking and financial institution systems, the Banking/Grid Logistics inventory ledger, Customer Management, Order Management, Inventory Management, Billing & Revenue Management, Financial Management, Commercial Contracts, regulatory systems, and other relevant enterprise applications. Integration shall support controlled exchange of financing notifications, approvals, facility positions, collateral status, stock status, entitlements, releases, transactions, and other CFA information, with interface monitoring, error handling, and traceability.		
CFA10	Reporting, Confirmations, Analytics & Auditability	The solution shall provide dashboards, reports, and configurable statements covering CFA status, financing utilization, available and utilized limits, financed, blocked and released stock, customer and financier exposure, collateral coverage, pending approvals, expiries, exceptions, and reconciliation status. It shall support automated preparation, validation, and controlled distribution of balance confirmation and financial position statements, with drill-down capability, historical records, and complete audit trails.		

2.2.4.2.6.7 Customer Self-Service & Digital Commercial Services

Overview

The proposed solution shall provide a secure, web-based and mobile-enabled Customer Self-Service Portal serving as the primary digital interface between the kPC and its customers. The portal shall enable authorized customers to register and manage accounts, submit and track orders, nominations and service requests, access inventory and entitlement information, monitor deliveries and transactions, exchange documents, view invoices and statements, receive notifications, and access authorized reports and commercial information. The portal shall integrate with O2C, Product Delivery, Inventory, Entitlement, CFA, Billing, Finance, Terminal and other relevant enterprise systems while providing secure access, workflow, auditability and real-time transaction visibility.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CSP01	Customer Registration, Authentication & Access Management	The solution shall provide secure customer registration, onboarding, identity verification, multi-factor authentication, user and organization profile management, role-based access, delegated authority, password management, and controlled account activation, suspension and deactivation.		
CSP02	Customer Account & Profile Management	The solution shall enable authorized customers to maintain organization details, authorized users, contacts, communication preferences and supporting information, subject to applicable approval and master-data governance controls.		
CSP03	Orders, Nominations & Service Requests	The solution shall enable customers to create, submit, amend, cancel and track authorized petroleum orders, nominations, product delivery requests, pipeline/terminal transfer requests, linefill requests, hydrant requests and other applicable commercial transactions, subject to configured validation and approval workflows.		
CSP04	Order & Delivery Visibility	The solution shall provide real-time visibility of order and nomination status, approvals, allocations, schedules, loading and delivery status, dispatched quantities, delivery confirmations, and other authorized operational events across the customer transaction lifecycle.		
CSP05	Inventory, Entitlement & Commercial Position	The solution shall provide customers with controlled visibility of applicable stock entitlements, allocations, inventory balances, linefill positions, financed/released stock where authorized, utilization, outstanding commitments and transaction history, sourced from the relevant authoritative enterprise systems.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
CSP06	Invoices, Statements & Payments	The solution shall provide secure access to invoices, credit/debit notes, account statements, charges, payment status and other authorized financial information, and shall support integration with billing, finance and payment platforms for applicable customer transactions.		
CSP07	Document & Certificate Management	The solution shall enable authorized customers and internal users to securely submit, validate, access, retrieve and manage applicable contracts, delivery documents, BOLs, FANs, quality certificates, invoices, statements, permits, confirmations, supporting evidence and other commercial or regulatory documents, with document-type validation, mandatory-document rules, version control, retention, access control and auditability.		
CSP08	Notifications, Alerts & Customer Communication	The solution shall provide configurable portal, email, SMS and other approved notifications to customers and relevant internal stakeholders for order submissions, approvals, schedule changes, delivery events, exceptions, reversal and correction requests, approval or rejection, execution, document availability, invoices, payments, account actions, entitlement changes and other relevant customer and commercial events. Notifications shall support configurable recipients, triggers, escalation rules and delivery status tracking.		
CSP09	Customer Workflow, Approvals & Digital Interaction	The solution shall support customer-side and authorized internal-user approvals, acknowledgements, electronic submissions, document attachments, digital signatures where applicable, delegated authority, escalation, and controlled amendment, reversal, correction and cancellation workflows, with configurable maker-checker controls, segregation of duties, multi-level authorization, and complete traceability of all actions.		
CSP10	Customer Reporting & Analytics	The solution shall provide configurable customer dashboards, transaction histories, order and delivery reports, inventory and entitlement statements, invoice and payment reports, utilization information and other authorized KPIs, with filtering, drill-down and export capabilities.		
CSP11	Customer Support, Reversals,	The solution shall enable customers and authorized internal users to raise, track and manage queries, complaints, claims,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Corrections & Exception Management	disputes, transaction exceptions, and requests for reversal or correction of authorized financial, operational, inventory and entitlement transactions. It shall support categorization, prioritization, validation, supporting-document submission and verification, configurable approval workflows, maker-checker controls, controlled execution, escalation, notifications, status tracking and resolution, with appropriate integration across O2C, Product Delivery, Inventory & Entitlement, Billing & Revenue Management, ERP/Finance and other affected systems to maintain transactional consistency and auditability.		
CSP12	Security, Privacy & Audit	The solution shall enforce encryption, role-based and least-privilege access, segregation of customer data, secure session management, audit logging, data protection and retention controls, and complete traceability of customer and system activities. Audit records shall capture, as applicable, the user or system actor, date/time, transaction or request reference, action performed, previous and new values, approvals, status changes, execution details and justification, and shall be protected against unauthorized alteration or deletion.		
CSP13	Enterprise Integration & Digital Services	The solution shall provide secure API-based integration with Customer Management, O2C and Product Delivery, Inventory & Entitlement Management, CFA Management, Billing & Revenue Management, Terminal Management, Queue & Yard Management, ERP/Finance, Document Management, Identity & Access Management, payment platforms, regulatory systems and enterprise analytics, ensuring synchronized and authoritative customer information.		

2.2.4.2.6.8 Pricing & Billing Management

The solution shall provide an integrated Pricing, Billing & Revenue Management capability to define and govern tariffs, calculate charges, validate billable transactions, generate invoices, manage payments and adjustments, and support revenue assurance for petroleum transportation, storage, throughput, terminal, hydrant, loading, pipeline, marine, and other authorized commercial services. The solution shall ensure accurate, transparent, auditable, and contract-compliant charging through effective-dated pricing, automated billing, tax compliance,

reconciliation, dispute management, and integration with operational, commercial, financial, banking, and regulatory systems.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
PBM01	Pricing & Tariff Management	The solution shall provide centralized management of tariffs, prices, charges, levies, discounts, rebates, penalties, and customer-specific or contract-based rates, supporting fixed, variable, tiered, volume-based, location-based, service-based, and other configurable pricing models. Pricing shall support effective dating, version control, validity periods, pricing hierarchies and precedence rules, multi-currency and tax-inclusive/exclusive configurations where applicable.		
PBM02	Pricing Rules & Charge Calculation	The solution shall provide a configurable, real-time pricing engine to automatically determine and calculate applicable charges based on product, customer, contract, service, quantity, location, logistics mode, transaction type, service period, storage duration, holding period, inventory ageing, and other approved business rules. It shall support surcharges, discounts, rebates, penalties, incentives, minimum charges, thresholds, customer-specific arrangements, and storage, holding, throughput, and ageing-based charges. The solution shall support pricing simulation, scenario analysis, and pre-billing calculation to validate pricing outcomes before billing or contract execution.		
PBM03	Contract & Commercial Pricing Control	The solution shall link approved contracts, agreements, service terms, and customer-specific commercial arrangements to applicable pricing rules, including validity periods, consumption or volume thresholds, service conditions, and negotiated rates. It shall enforce approved pricing hierarchies and precedence rules and prevent conflicting, expired, incomplete, duplicate, or unauthorized pricing configurations. The solution shall provide configurable validation and consistency checks covering pricing completeness, overlapping validity periods, duplicate definitions, conflicting rules, and other pricing integrity conditions, with controlled exception handling and alerts.		
PBM04	Billing & Invoice Management	The solution shall support end-to-end billing from validated billable events through billing runs, invoice calculation, validation, approval, issuance, electronic distribution, amendment, cancellation, reversal, credit notes, debit notes, and reissuance. It shall support individual, consolidated, customer-based, contract-based, service-based, depot-based, and multi-service billing, together with daily, weekly, monthly, periodic, and event-driven billing cycles. The solution shall support defined billing cut-off rules, billing-period opening, locking and closure, controlled		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		billing-run execution, and ageing-based billing for storage, holding, and other applicable inventory-related charges. All invoices shall maintain complete linkage to underlying operational transactions, validated quantities, applicable pricing, contracts, and commercial records. The solution shall support electronic invoice distribution through customer portals, email, secure channels, APIs, e-invoicing platforms, and other authorized channels, with delivery-status tracking.		
PBM05	Taxation, E-Invoicing & Statutory Compliance	The solution shall automatically apply applicable taxes, statutory levies, withholding taxes, regulatory fees, and other statutory charges based on configured rules and applicable legislation. It shall support compliant electronic invoicing, tax documentation, and integration with relevant tax and regulatory platforms for validation, submission, and reporting.		
PBM06	Payment, Receivables & Settlement Management	The solution shall support recording, matching, allocation, reconciliation, and settlement of customer payments, advances, deposits, partial payments, refunds, write-offs, and other financial adjustments. It shall provide visibility of outstanding balances, receivables ageing, payment status, and customer account positions, with integration to banking and financial systems.		
PBM07	Billing Validation, Reconciliation & Dispute Management	The solution shall provide pre- and post-billing validation and reconciliation of billable transactions against orders, contracts, pricing, inventory, entitlements, custody-transfer quantities, ATG, SCADA, metering, terminal, and other operational records. It shall support duplicate detection, completeness checks, configurable tolerances, variance investigation, billing disputes, claims, adjustments, reversals, escalation, and controlled resolution workflows.		
PBM08	Revenue Assurance & Recognition	The solution shall provide revenue assurance controls to identify missing or incomplete billable events, pricing errors, unauthorized charges, revenue leakage, duplicate billing, under-billing, over-billing, and reconciliation discrepancies. It shall support configurable revenue recognition rules aligned with applicable accounting requirements, custody-transfer events, service completion, billing events, and contractual obligations, with automated posting or integration to the General Ledger and financial systems.		
PBM09	Billing Governance, Workflow & Audit	The solution shall support configurable maker-checker workflows, delegated authority, segregation of duties, billing-period controls, approvals, notifications, exception handling, and controlled billing adjustments. It shall provide automated notifications and alerts for billing runs, invoice		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		generation, approvals, invoice dispatch, payment due dates, overdue invoices, failed transactions, disputes, adjustments, and other configured billing events. The solution shall maintain complete, immutable audit trails covering pricing changes, calculations, billing runs, invoices, approvals, adjustments, payments, disputes, reconciliations, revenue postings, and regulatory submissions, together with secure document management, retention, version control, and controlled access.		
PBM10	Integration, Reporting & Analytics	The solution shall integrate with Customer Management, Order-to-Cash, Product Delivery, Inventory & Entitlement Management, Terminal Management, Planning & Scheduling, Commercial Contracts, Financial Management/ERP, Customer Self-Service Portal, banking and payment platforms, tax and regulatory systems, and enterprise reporting platforms through secure APIs and controlled interfaces. The solution shall expose approved pricing and charge-calculation services through secure APIs for consumption by billing, order management, entitlement, inventory, simulation, reporting, and other authorized systems. It shall provide dashboards and analytics covering tariffs, active and expired pricing, pending approvals, pricing impacts, billing status, revenue, receivables, payment ageing, customer profitability, service-wise revenue, reconciliation, disputes, revenue leakage, pricing variances, historical pricing changes, revenue and margin trends, customer pricing behaviour, tariff utilization, and key commercial KPIs, with drill-down and audit traceability.		

2.2.4.2.6.9 Quantity Conversion & Standardization Management

Overview

The solution shall provide an integrated Quantity Conversion & Standardization Management capability to capture, calculate, validate, standardize, and reconcile petroleum quantities across the supply chain. The solution shall support industry-recognized petroleum measurement standards, temperature, pressure and density corrections, mass and volume conversions, custody-transfer calculations, inventory reconciliation, configurable measurement rules, and regulatory and commercial reporting, with full traceability of measurement inputs, conversion factors, calculations, and adjustments.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
QCM01	Measurement & Quantity Capture	The solution shall capture and validate petroleum measurement data from approved sources including custody-transfer meters, flow computers, Automatic Tank Gauging (ATG), tank measurements, weighbridges, SCADA, vessel		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		systems, LPG systems, and other authorized measurement devices, retaining the source, timestamp, measurement basis, and relevant operating conditions.		
QCM02	Quantity Conversion & Standardization	The solution shall support standardized quantity determination and conversion across applicable petroleum products, including crude oil, refined products, black products, and LPG, covering observed volume, gross volume, net volume, Gross Standard Volume (GSV), Net Standard Volume (NSV), mass, and other configured measurement units.		
QCM03	Correction Factors & Measurement Standards	The solution shall apply configurable, product-specific temperature, pressure, density, and other correction factors using approved petroleum measurement standards, conversion tables, calibration parameters, and reference conditions. Standards and calculation parameters shall be version-controlled and effective-dated.		
QCM04	Calculation, Validation & Reconciliation	The solution shall perform traceable quantity calculations and validate standardized quantities against operational transactions, inventory movements, pipeline transfers, marine receipts, tank movements, loading and delivery transactions, and custody-transfer records. It shall identify variances, apply configurable tolerances, and support controlled investigation and adjustment.		
QCM05	Exception & Variance Management	The solution shall detect and manage incomplete, inconsistent, or anomalous measurement data, including missing or invalid density, temperature or pressure inputs, metering discrepancies, calibration deviations, and conversion failures. It shall support configurable alerts, investigation, escalation, approval, and resolution workflows.		
QCM06	Measurement Configuration & Governance	The solution shall provide configurable product parameters, conversion rules, measurement units, correction tables, tolerance limits, reference conditions, calibration parameters, and regulatory or contractual factors without requiring software changes. It shall enforce controlled access, maker-checker approval, segregation of duties, and effective-dated version control.		
QCM07	Custody Transfer, Inventory & Commercial Integration	The solution shall provide a consistent quantity basis for custody transfer, inventory accounting, entitlement management, reconciliation, pricing and billing, and commercial settlement across marine, pipeline, terminal, tank, truck, wagon, hydrant, pump-over, and LPG operations. Approved conversion logic shall be consistently		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		applied across integrated operational and enterprise systems.		
QCM08	Audit, Compliance & Traceability	The solution shall maintain complete and reproducible audit trails for all quantity calculations, including source measurements, input conditions, correction factors, standards, conversion methodology, calculation results, overrides, approvals, and adjustments. It shall support recognized petroleum measurement standards, contractual requirements, regulatory reporting, calibration records, inspections, and dispute resolution.		
QCM09	Reporting & Analytics	The solution shall provide configurable quantity, custody-transfer, conversion, reconciliation, measurement variance, and operational reporting, including dashboards, KPIs, trends, historical analysis, and drill-down from standardized quantities to underlying measurements and calculation parameters.		
QCM10	Integration & Data Exchange	The solution shall integrate through secure APIs and controlled interfaces with Inventory & Stock Management, Terminal Management, Order-to-Cash & Product Delivery, Pricing & Billing, Quality Management, Financial Management, SCADA, ATG, custody-transfer and mainline metering systems, flow computers, vessel systems, LPG systems, and enterprise analytics and reporting platforms.		

2.2.4.2.6.10 Master Data Governance & Management

Overview

The solution shall provide a centralized Master Data Governance capability establishing a single, authoritative source of truth for master data used across planning, scheduling, execution, inventory, billing, reporting, reconciliation, and commercial processes. The solution shall provide secure self-service capabilities for authorized transporters and fleet operators to submit and maintain transporter, truck, trailer, compartment, and driver master data, upload supporting documentation, initiate amendments and renewals, and track submission and approval status, subject to configured validation, workflow, and authorization controls.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MDM01	Product Master	The solution shall provide centralized management of product/material master data, including product codes, names, grades, categories, specifications, quality attributes, units of measure, regulatory classifications, product compatibility, and commercial applicability, with controlled lifecycle management.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MDM02	Terminal/Depots Master	The solution shall provide centralized management of depot, terminal, station, and facility master data, including identification, location, ownership, operational status, capacities, services, operating constraints, connected assets, and applicable product capabilities.		
MDM03	Tank Master & Strapping Tables	The solution shall provide centralized management of tank master data, including tank identification, location, capacity, product compatibility, operating limits, measurement configuration, associated depot/terminal, and status, and shall support controlled creation, validation, approval, versioning, effective dating, and maintenance of tank strapping/calibration tables used for level-to-volume conversion and inventory measurement.		
MDM04	Pipeline Master	The solution shall provide centralized management of pipeline and segment master data, including identifiers, routes, connected facilities, capacities, products handled, operating constraints, ownership, and operational status.		
MDM05	Vessel & Marine Master	The solution shall provide centralized management of vessel and marine asset master data, including vessel identification, owner/operator, capacity, class, product compatibility, regulatory information, berth compatibility, operating constraints, and status.		
MDM06	Customer Master	The solution shall provide centralized management of Oil Marketing Companies (OMCs), Importers/Marketers and other applicable petroleum customers, including identification, legal and KYC information, customer classification, contractual and operational attributes, applicable products, delivery relationships, credit profile where applicable, regulatory/compliance status, and lifecycle status. It shall support controlled customer onboarding and multi-stage legal, financial, technical, and compliance vetting, with customer activation permitted only following completion and approval of applicable onboarding requirements.		
MDM07	Destination / Ship-to-Party Master	The solution shall provide centralized management of destination and ship-to-party master data, including identification, customer association, physical location, delivery address, terminal/depot association, applicable products, delivery constraints, authorization status, and operational validity.		
MDM08	Partner Terminal Master	The solution shall provide centralized management of partner-country and third-party terminal master data, including identification,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		location, owner/operator, storage capacity, product capabilities, connected infrastructure, operating constraints, commercial relationships, and status.		
MDM09	Transporter Master	The solution shall provide centralized management of transporter/carrier master data, including identification, ownership, contact details, fleet association, authorization and contractual status, compliance information, service scope, and operational status.		
MDM10	Truck, Trailer & Compartment Master	The solution shall provide centralized management of prime mover, trailer, tanker, and compartment master data, including registration, ownership, transporter association, configuration, capacity, product compatibility, operational status, and compartment-level calibration data.		
MDM11	Driver Master	The solution shall provide centralized management of driver master data covering the complete lifecycle, including identity, transporter association, licence and class, issuing authority, endorsements, certifications, work permits where applicable, compliance credentials, validity and expiry dates, operational eligibility, and status.		
MDM12	Transporter, Truck & Driver Compliance	The solution shall support management and validation of applicable transporter, vehicle, and driver compliance requirements, including licences, registration, roadworthiness, insurance, hazardous-cargo permits, certifications, and other regulatory credentials, with expiry monitoring, alerts, renewal workflows, and restrictions on non-compliant records.		
MDM13	Regulatory & External Validation	The solution shall integrate with applicable regulatory and external systems, including EPRA where interfaces are available, to validate relevant customer, transporter, vehicle, driver, and other master-data attributes and compliance status, and shall flag or restrict non-compliant records in accordance with configured business rules.		
MDM14	Compartment Calibration & Loading Configuration	The solution shall maintain approved compartment-level calibration, capacity, product compatibility, and loading configuration data and ensure that validated data is available to loading, quantity calculation, inventory reconciliation, and related operational processes.		
MDM15	Commercial & Credit Master Data	The solution shall provide centralized management of commercial and credit master data, including customer contracts and agreements, pricing agreements, tariffs, service charges, penalties, payment terms, customer-specific pricing, credit limits, exposure thresholds, risk classifications, and validity periods, with		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		effective-date control and versioning. It shall support contract creation, approval, amendment, renewal, suspension, and termination, and enforce linkage of approved commercial terms to applicable orders, nominations, allocations, deliveries, billing, and other operational processes. The solution shall support configurable credit blocking, unblocking, exposure thresholds, and authorized overrides.		
MDM16	Master Data Workflow, Onboarding & Lifecycle Management	The solution shall provide configurable workflows for master-data creation, customer onboarding and vetting, submission, validation, maker-checker review, approval, activation, amendment, suspension, rejection, deactivation, retirement, and reactivation. It shall support configurable roles, approval levels, escalation, segregation of duties, and activation controls to ensure that customers and other governed master-data records cannot be used in applicable commercial or operational transactions until all required approvals and validations have been completed.		
MDM17	Master Data Validation & Quality	The solution shall provide configurable validation, duplicate detection, completeness, consistency, and business rules to prevent invalid, incomplete, duplicate, conflicting, or unauthorized master-data records and shall provide data-quality monitoring covering completeness, accuracy, consistency, validity, and timeliness.		
MDM18	Document Management Integration	The solution shall integrate with the enterprise Electronic Document and Records Management System (eDRMS) to store, retrieve, manage, and retain documents associated with master-data records, including KYC documents, licences, certificates, strapping/calibration certificates, insurance, contracts, compliance records, driver credentials, and vehicle documentation, while maintaining document associations, expiry status, access controls, and audit traceability.		
MDM19	Master Data Integration & Distribution	The solution shall provide controlled synchronization and distribution of approved master data with enterprise, operational, regulatory, and external systems, including SAP, SCADA, tank management/tank gauging, stock management, vessel management, loading systems, ANPR/RFID, billing systems, and applicable regulatory platforms.		
MDM20	Security, Audit & Version Control	The solution shall enforce role-based access control and segregation of duties and maintain a complete audit trail and version history of master-data transactions, including user, date/time,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		action, previous and new values, approvals, status changes, effective dates, and applicable supporting information.		
MDM21	Master Data Monitoring & Reporting	The solution shall provide dashboards, alerts, and reports covering master-data health, pending approvals, duplicates, validation exceptions, expired credentials, non-compliant drivers and vehicles, inactive records, data-quality KPIs, master-data changes, and governance performance.		

2.2.4.2.6.11 Planning, Operational Reporting, Audit & Analytics

Overview

The solution shall provide an integrated reporting, audit, and analytics capability covering planning, scheduling, execution, inventory, marine, pipeline, terminal, loading, quality, commercial, reconciliation, and regulatory processes. The solution shall provide real-time dashboards, management and statutory reports, KPI analytics, drill-down capabilities, audit trails, data lineage, governed report generation and distribution, and secure retention of reporting and operational records.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
RPT01	Planning & Performance Reporting	The solution shall provide planning and scheduling reports comparing planned, nominated, scheduled, and actual activities, quantities, resources, capacity utilization, service levels, and performance, including deviations and exceptions.		
RPT02	Inventory & Reconciliation Reporting	The solution shall provide automated stock, gain/loss, outturn, and variance calculation and reconciliation across depots, terminals, pipelines, facilities, and enterprise level, covering all logistics modes and stock movements. It shall use validated data from ERP, inventory, ATG, SCADA, metering, surveyor, laboratory, physical measurement, and operational systems, with configurable gain/loss methodologies, thresholds, tolerances, and business rules by product, facility, logistics mode, customer, and reporting period.		
RPT03	Movement & Custody Reporting	The solution shall provide reports for marine, pipeline, inter-terminal, pump-over, mainline, truck, LPG, hydrant, and other product movements, including quantities, custody-transfer references, quantity conversions, approvals, QC results, and reconciliation outcomes.		
RPT04	Marine & Terminal Performance Reporting	The solution shall provide marine and terminal performance reports covering vessel and berth utilization, turnaround times, throughput, loading/discharge performance, demurrage exposure, operational efficiency, delays, and exceptions.		
RPT05	Delivery & Customer	The solution shall provide delivery and customer performance reports covering order fulfillment,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Performance Reporting	quantities delivered, destinations, delivery status, turnaround times, service levels, exceptions, and customer-related KPIs.		
RPT06	Quality & Compliance Reporting	The solution shall incorporate laboratory and quality results, product release status, density, contamination checks, JIG requirements, inspections, certifications, and other applicable compliance information into relevant operational, custody, inventory, and regulatory reports.		
RPT07	Asset & Maintenance Reporting	The solution shall provide reports covering tank integrity, inspections, calibration and strapping-table changes, maintenance activities, pipeline PIG operations, equipment status, and associated operational events and approvals.		
RPT08	Operational Event & Audit Reporting	The solution shall maintain and report time-stamped operational events and audit records, including meter and ATG readings, alarms, valve states, operator actions, approvals, safety checks, loading, transfers, overrides, exceptions, and manual entries.		
RPT09	Dashboards & Analytics	The solution shall provide real-time and historical dashboards and analytics for planning, operations, inventory, movements, quality, assets, commercial performance, reconciliation, and management KPIs, with configurable thresholds, alerts, trends, and visualizations.		
RPT10	Drill-Down & Data Lineage	The solution shall provide drill-down and drill-through from reports, dashboards, and KPIs to underlying transactions and source data, with end-to-end lineage to ERP, MDM, ATG, SCADA, metering, QC/LIMS, operational systems, and authorized manual entries.		
RPT11	Data Quality & Report Validation	The solution shall apply configurable data-quality and validation controls before report generation or publication, including completeness, consistency, anomaly, reconciliation, tolerance, and exception checks.		
RPT12	Regulatory & Statutory Reporting	The solution shall support generation, approval, and controlled submission of statutory and regulatory reports from validated datasets, including applicable KRA, EPRA, and other regulatory requirements.		
RPT13	Report Governance & Security	The solution shall provide role-based access, segregation of duties, report versioning, approval workflows, controlled publication, and configurable visibility for operational, commercial, finance, management, customer, audit, and regulatory users.		
RPT14	Report Scheduling & Distribution	The solution shall support scheduled, event-driven, and on-demand report generation and distribution in configurable formats, including PDF, Excel, CSV, and API-based feeds.		
RPT15	Audit, Retention & Archival	The solution shall maintain tamper-evident audit trails and secure retention, archival, and retrieval of reports, analytics outputs, operational logs, and audit records in		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		accordance with regulatory and organizational requirements, including integration with the enterprise eDRMS where applicable.		

2.2.4.2.6.12 Integration

Overview

The solution shall provide a secure, scalable, highly available, and resilient integration framework for reliable exchange of operational, commercial, inventory, financial, regulatory, and master data across internal and external systems. The framework shall support real-time, near-real-time, and batch integration while providing secure connectivity, interoperability, monitoring, exception handling, auditability, and controlled interface lifecycle management.

1.2. Systems Integration

Overview

The solution shall provide a secure, scalable, highly available, and resilient integration framework for reliable exchange of operational, commercial, inventory, financial, regulatory, and master data across internal and external systems. The framework shall support real-time, near-real-time, and batch integration while providing secure connectivity, interoperability, monitoring, exception handling, auditability, and controlled interface lifecycle management.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
INT01	Tank & Inventory Integration	The solution shall integrate with Automatic Tank Gauging (ATG), tank management, and inventory systems to receive tank levels, temperatures, water levels, product quantities, stock movements, and inventory status for stock accounting, reconciliation, monitoring, and reporting.		
INT02	Terminal & Loading Systems Integration	The solution shall integrate with terminal automation, loading control, Hydrant Management Systems, metering, and industrial control platforms to exchange approved operational instructions, transaction data, execution status, equipment status, and operational events, without directly controlling field equipment.		
INT03	Quality & Laboratory Integration	The solution shall integrate with Quality Control and Laboratory Information Management Systems (LIMS) to receive laboratory results, density, quality certificates, contamination assessments, product release status, and clearance confirmations for operational, inventory, and compliance processes.		
INT04	Metering & Custody Transfer Integration	The solution shall integrate with AccuLoad version 3/4, custody-transfer meters, flow meters, dispenser meters, and other metering systems to receive validated quantities, flow data, loading completion information, and custody-transfer measurements for quantity reconciliation, stock accounting, billing, and reporting.		
INT05	SCADA & Operational	The solution shall integrate with SCADA, Leak Detection Systems (LDS), condition-monitoring,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
	Monitoring Integration	and equipment-monitoring platforms to receive alarms, leak alerts, pressure conditions, equipment status, and operational events for monitoring, escalation, analysis, and audit purposes.		
INT06	Truck, Gate & Mobility Integration	The solution shall integrate with ANPR (primary vehicle identification), RFID (secondary identification), truck management, and transportation systems to support vehicle and driver identification, access validation, movement tracking, loading authorization, and operational visibility.		
INT07	Marine & Port Integration	The solution shall integrate with port, marine, vessel, and logistics management systems to support vessel nominations, berth scheduling, cargo coordination, marine operations, shipment execution, and status visibility.		
INT08	Regulatory & Customs Integration	The solution shall integrate with regulatory, customs, and taxation platforms, including KRA iCMS, EPRA, NTSA, and other applicable authorities, to exchange validated transactions, cargo manifests, Bills of Lading, declarations, licensing information, compliance data, statutory reports, acknowledgements, and regulatory status updates.		
INT09	Enterprise & Commercial Integration	The solution shall integrate with ERP, SAP, finance, billing, procurement, customer management, and enterprise reporting systems to support financial postings, invoicing, revenue accounting, customer transactions, and synchronization of applicable master and reference data.		
INT10	Master Data Synchronization	The solution shall provide controlled synchronization and distribution of approved master data between the authoritative MDM capability and integrated systems, including products, depots/terminals, tanks, pipelines, vessels, customers, destinations/ship-to parties, partner terminals, transporters, trucks, drivers, locations, and other applicable operational master data.		
INT11	Integration Methods & Standards	The solution shall support open, industry-standard integration mechanisms, including REST/SOAP APIs, web services, messaging, file-based exchange, and event-driven integration, supporting real-time, near-real-time, and batch processing.		
INT12	Integration Orchestration & Transformation	The solution shall support configurable integration orchestration, routing, transformation, validation, enrichment, mapping, filtering, sequencing, acknowledgement, and status synchronization across heterogeneous systems.		
INT13	Integration Security	The solution shall provide configurable integration security controls, including authentication, authorization, encryption, secure communication		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		protocols, API security, digital certificates, key and credential management, and non-repudiation where required.		
INT14	Integration Monitoring & Administration	The solution shall provide centralized monitoring and administration of integrations, including interface health, message and transaction tracking, processing status, throughput, latency, availability, service-level performance, and operational dashboards.		
INT15	Exception & Recovery Management	The solution shall support automated error handling, retry, queuing, replay, recovery, reconciliation, escalation, and notification for failed, delayed, rejected, duplicate, or incomplete integration transactions.		
INT16	Integration Audit & Traceability	The solution shall maintain complete audit trails for inbound and outbound integration transactions, including transaction identifiers, timestamps, source and destination systems, payload references, acknowledgements, processing status, transformations, errors, and relevant user or system actions.		
INT17	High Availability & Business Continuity	The solution shall support high availability, fault tolerance, disaster recovery, and business continuity for critical integrations, including message queuing, persistent buffering, failover, replay, recovery, and controlled reprocessing following system or communication failures.		
INT18	Interface Lifecycle & Version Management	The solution shall support interface versioning, configuration management, dependency tracking, lifecycle management, backward compatibility, and controlled deployment of integration changes to minimize operational disruption.		
INT19	Integration Performance & SLA Reporting	The solution shall provide integration performance analytics and reporting covering transaction volumes, processing times, response times, interface availability, failures, retries, latency, throughput, and service-level compliance.		

2.2.4.2.7 Terminal Management System

The proposed solution shall provide an integrated Terminal Management System (TMS) for the end-to-end management of petroleum terminal operations, covering terminal operations, truck loading, loading safety and compliance, and vehicle identification (ANPR primary, RFID secondary). The solution shall provide real-time visibility and controlled execution of product receipt, storage, transfer, loading, dispatch, and truck movements; integrate with SCADA, TAS, ATG, metering, loading automation, ERP, inventory, quality, security, and regulatory systems; optimize terminal throughput and truck turnaround; enforce safety and compliance controls; and maintain complete transaction traceability, auditability, and operational accountability.

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
TMS01	Terminal Management	The solution shall support end-to-end management of terminal operations including product receipt, storage, transfers, blending, inventory, tank and ullage management, custody transfer, product segregation, operational workflows, inspections, exception management, regulatory compliance, reporting, and integration with SCADA, ATG, metering, LIMS, pipeline, vessel, ERP, and other enterprise systems.		
TMS02	Truck Loading Management	The solution shall support end-to-end truck and wagon loading management, including customer orders and nominations, entitlement and product validation, loading authorization, vehicle and driver verification, loading bay allocation, loading execution, quantity capture, quality clearance, BOL/FAN generation, inventory posting, reconciliation, shipment documentation, gate release, and integration with TAS, AccuLoad version 3/4, Tankage, Stock Management, LIMS, KRA ICMS, billing, and related systems.		
TMS03	Queue & Yard Management	The solution shall provide real-time management of truck appointments, queues, staging areas, yard occupancy, loading slots, bay allocation, truck movement, traffic flow, congestion, prioritization, and resource utilization, with configurable scheduling and queue rules, customer/transporter visibility, notifications, exception handling, offline continuity, and integration with ANPR, loading, terminal, and access-control systems.		
TMS04	Smart Gate Integration	N/A		
TMS05	Automatic Number Plate Recognition (ANPR) Integration	The solution shall support integration to ANPRs for vehicle identification and movement tracking		
TMS06	**Loading Safety & Compliance Management**	The solution shall provide centralized safety and compliance controls for truck loading, including grounding, overfill protection, loading permissive, safety interlocks, vehicle positioning, wheel chocks, compartment readiness, emergency shutdown integration, safety-device monitoring, controlled overrides, loading completion safety checks, incident and		

Code	Functional Area	Functional Requirement	Tenderers Response (Yes/No)	Evidence Page
		environmental event recording, compliance verification, audit trails, dashboards, and reporting in accordance with applicable safety and industry standards.		

2.2.4.2.8 Quality Control Management

Overview

The proposed solution shall provide an integrated Quality Control Management capability to plan, execute, monitor, validate, and govern petroleum product quality across receipt, storage, transportation, blending, transfer, loading, and dispatch, ensuring end-to-end traceability of sampling, testing, inspections, quality decisions, certifications, product release, non-conformances, and corrective actions. The solution shall ensure compliance with applicable product specifications, industry standards, regulatory requirements, and organizational quality policies, while integrating with laboratory, operational, inventory, metering, planning, terminal, document management, enterprise, and regulatory systems to ensure only validated and approved quality information is used for operational and product-release decisions.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
QC01	Quality Planning & Inspection	The solution shall support planning, scheduling, execution, and monitoring of quality inspections, sampling plans, testing schedules, inspection checklists, and quality-control activities across terminals, pipelines, marine operations, tanks, batches, trucks, and other applicable facilities.		
QC02	Sampling & Laboratory Management	The solution shall support end-to-end sample management, including sample registration, unique identification, classification, acceptance, preservation, chain-of-custody, routing, test assignment, execution, retesting, retention, and disposal, with traceability to the originating product, batch, tank, cargo, movement, or vehicle.		
QC03	Quality Standards & Validation	The solution shall maintain controlled and versioned product specifications, test methods, quality standards, regulatory requirements, and applicable contractual limits, and shall validate laboratory and inspection results against configured specifications, tolerances, validity periods, and quality rules.		
QC04	Quality Decision & Product Release	The solution shall support controlled quality decisions, including pass, conditional release, fail, quarantine, rejection, and recertification for cargoes, tanks, batches, trucks, and product movements, ensuring release is permitted only after completion and approval of applicable quality requirements.		
QC05	Quality Certificates & Documentation	The solution shall generate, approve, digitally sign, distribute, version, and retain applicable quality documentation, including Certificates of Analysis (CoA), Certificates of Quality (CoQ), tank and truck		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		release certificates, laboratory reports, inspection reports, and compliance certificates, with traceability to approved source data.		
QC06	Non-Conformance & CAPA	The solution shall support identification, classification, containment, investigation, root-cause analysis, resampling, retesting, quarantine, disposition, corrective and preventive actions (CAPA), escalation, approval, effectiveness verification, and closure of quality non-conformances, including contamination and specification deviations.		
QC07	Product & Batch Traceability	The solution shall provide end-to-end traceability of product quality by product, batch, cargo, tank, pipeline movement, sample, test result, inspection, transfer, loading, and customer delivery, including linkage between quality results and associated quantities and transactions.		
QC08	Quality Assurance & Governance	The solution shall provide configurable quality workflows, maker-checker controls, segregation of duties, delegated authority, electronic approvals, notifications, controlled overrides, document attachments, and comprehensive audit trails for quality activities and decisions.		
QC09	Operational Quality Advisory	The solution shall generate configurable quality advisories using validated laboratory and operational data to support interface cutting, slop management, offloading, blending, density adjustment, re-injection, and other applicable quality-related operational decisions, with approval, acknowledgement, escalation, and execution tracking.		
QC10	Customer Laboratory Services	The solution shall support controlled customer laboratory testing services, including self-service test requests, sample submission, test selection, supporting documentation, request validation, testing, SLA monitoring, result approval, certificate issuance, secure result publication, and customer access to historical results.		
QC11	Quality Reporting & Analytics	The solution shall provide configurable dashboards, reports, and analytics covering quality trends, laboratory workload and turnaround time, product quality, density, interfaces, contamination, OOS trends, batch quality, compliance, non-conformances, CAPA, certification, and quality performance, with drill-down to underlying records.		
QC12	Regulatory Compliance & Audit	The solution shall support compliance with applicable petroleum, aviation-fuel, laboratory, environmental, contractual, and regulatory requirements, including relevant ASTM, ISO, JIG, AFQRJOS, KS/EAS, EPRA, NEMA, and other applicable standards and requirements, with controlled standards, audit evidence, inspection history, and compliance reporting.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
QC13	Quality Data Governance	The solution shall enforce data validation, completeness, consistency, authorization, version control, and controlled use of quality information, including prevention of unauthorized modification or use of unapproved laboratory results, specifications, certificates, and quality decisions.		
QC14	Systems Integration & Data Exchange	The solution shall integrate with applicable laboratory/LIMS, Operations, Planning & Scheduling, Inventory, Terminal Management, Tank Gauging/ATG, SCADA, metering, loading, marine, ERP/SAP, Customer Management, eDRMS, Asset Management, analytics, and regulatory systems to exchange samples, test requests, operational data, results, certificates, quality decisions, alerts, and advisories.		
QC15	Integration Monitoring & Traceability	The solution shall provide controlled and auditable integration using APIs, web services, messaging, file-based, or event-driven mechanisms, with interface validation, monitoring, error handling, retry, alerting, reconciliation, source identification, timestamps, and end-to-end data lineage.		
QC16	Security, Audit & Records Management	The solution shall enforce role-based access, segregation of duties, electronic signatures, secure records management, and comprehensive audit trails covering sample handling, testing, result changes, approvals, overrides, quality decisions, certificates, releases, and system transactions, with retention and archival in accordance with applicable requirements.		

2.2.4.2.9 Shared Services

2.2.4.2.9.1 Integrated Development Platform (IDP)

Overview

The proposed solution shall provide an Integrated Development Platform (IDP) that enables the Corporation to develop, configure, customize, extend, integrate, deploy, and manage enterprise applications and business processes while preserving the integrity of the core ERP solution. The platform shall provide enterprise middleware capabilities including API management, Enterprise Service Bus (ESB), service orchestration, data transformation, event-driven integration, messaging, workflow automation, DevOps, application lifecycle management, and secure interoperability between enterprise applications, operational technologies, cloud services, and external systems.

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
IDP01	Application Development	The solution shall support development of enterprise applications using low-code, no-code, and professional development tools, reusable components, visual designers, code editors, templates, and application frameworks.		

IDP02	Application Configuration and Customization	The solution shall support configuration and extension of business processes, forms, dashboards, workflows, validations, business rules, reports, and user interfaces without modifying the core ERP application.		
IDP03	Workflow and Business Process Automation	The solution shall support graphical workflow design, business process automation, approvals, notifications, escalations, service orchestration, event-driven processes, robotic process automation (RPA), and business rules management.		
IDP04	Enterprise Middleware and Service Bus (ESB)	The solution shall provide enterprise middleware capabilities including an Enterprise Service Bus (ESB), service orchestration, message routing, message transformation, protocol mediation, enterprise messaging, publish-subscribe communication, asynchronous processing, guaranteed message delivery, and reliable communication between enterprise applications and external systems.		
IDP05	API Management and Integration Services	The solution shall support API development, REST, SOAP, GraphQL, OData, API Gateway, API publishing, API lifecycle management, API security, API monitoring, webhooks, service virtualization, and secure integration with internal and external applications.		
IDP06	Data Integration and Transformation	The solution shall support ETL/ELT processes, data mapping, transformation, validation, synchronization, migration, master data synchronization, batch processing, real-time integration, and data quality management.		
IDP07	Event Streaming and Messaging	The solution shall support event-driven architecture, enterprise messaging, message queues, publish-subscribe messaging, event streaming, message persistence, event notifications, asynchronous communication, and integration with IoT and operational systems.		
IDP08	Integration Connectors	The solution shall provide configurable connectors, adapters, and integration templates for ERP modules, SCADA, PLCs, IoT devices, databases, cloud platforms, banking systems, payment gateways, government systems, enterprise applications, and third-party services.		

IDP09	Application Lifecycle Management	The solution shall support source code management, version control, environment management, configuration management, release management, deployment pipelines, rollback, change management, and application lifecycle governance.		
IDP10	DevOps and Continuous Delivery	The solution shall support Continuous Integration (CI), Continuous Delivery (CD), automated builds, automated testing, deployment automation, release orchestration, environment promotion, infrastructure as code, and DevOps pipeline management.		
IDP11	Security and Identity Integration	The solution shall support role-based access control, Single Sign-On (SSO), Multi-Factor Authentication (MFA), OAuth, OpenID Connect, API security, encryption, digital certificates, secrets management, audit trails, and secure application development practices.		
IDP12	Monitoring and Operational Analytics	The solution shall support monitoring of applications, APIs, integrations, workflows, middleware services, message queues, system performance, logging, diagnostics, alerts, operational dashboards, usage analytics, and platform health monitoring.		
IDP13	Mobile, Portal and User Experience Development	The solution shall support development of responsive web portals, mobile applications, offline capabilities, configurable dashboards, multilingual interfaces, accessibility standards, reusable UI components, and omnichannel user experiences.		
IDP14	AI-Assisted Development	The solution shall support AI-assisted code generation, workflow recommendations, automated documentation, intelligent debugging, code optimization, predictive development assistance, chatbot integration, and developer productivity tools.		
IDP15	Integration Governance	The solution shall support centralized governance of integrations, APIs, services, middleware components, reusable assets, integration catalogues, policy enforcement, service versioning, dependency management, compliance monitoring, and complete auditability.		

IDP16	Integration and Governance	The solution shall integrate seamlessly with all ERP modules, Operational Technology (SCADA, PLCs, ATG), Enterprise Service Bus, Identity & Access Management, Enterprise Document & Records Management, AI & Analytics, Business Intelligence, cloud platforms, mobile applications, third-party systems, government platforms, banking systems, and external APIs while enforcing enterprise security, interoperability, scalability, and comprehensive auditability.		

2.2.4.2.9.2 Workflow and Business Process Automation

Overview

The proposed solution shall provide an integrated Workflow & Business Process Automation capability to design, execute, monitor, and optimize enterprise business processes across the Corporation. The solution shall support low-code/no-code workflow development, process orchestration, business rules management, case management, approvals, notifications, and robotic process automation (RPA) to improve operational efficiency, standardize business processes, enhance governance, and accelerate digital transformation.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
WBPA01	Workflow Design and Automation	The solution shall support graphical design, configuration, deployment, execution, and lifecycle management of configurable business workflows, approval processes, service requests, and operational procedures without extensive software development.		
WBPA02	Business Process Orchestration	The solution shall support orchestration and automation of end-to-end business processes across multiple enterprise applications, departments, business units, and external stakeholders while maintaining process visibility and control.		
WBPA03	Business Rules Management	The solution shall provide configurable business rules, decision tables, validation rules, routing logic, service-level agreements (SLAs), escalation rules, and conditional processing to automate business decisions and ensure policy compliance.		
WBPA04	Forms and Case Management	The solution shall support creation and management of electronic forms, dynamic data capture, case management, document attachments, task assignments, collaboration, and lifecycle management of business cases and requests.		
WBPA05	Task Management and Notifications	The solution shall support automated task assignment, work queues, reminders, escalations, notifications, delegation, workload balancing, and monitoring of pending and completed workflow activities.		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
WBPA06	Robotic Process Automation (RPA)	The solution shall support integration with Robotic Process Automation technologies to automate repetitive, rule-based tasks across enterprise applications while providing centralized management, monitoring, and auditability of software robots.		
WBPA07	Workflow Governance and Audit	The solution shall support configurable approval hierarchies, delegated authority, electronic approvals, audit trails, process versioning, workflow history, electronic records, and complete traceability of all workflow activities.		
WBPA08	Process Monitoring and Analytics	The solution shall provide configurable dashboards, workflow performance reports, SLA monitoring, bottleneck analysis, process efficiency metrics, executive dashboards, KPI monitoring, trend analysis, and self-service reporting with drill-down capabilities.		
WBPA09	Process Optimization and Continuous Improvement	The solution shall support process mining, workflow optimization, bottleneck identification, performance benchmarking, continuous improvement initiatives, simulation of process changes, and recommendations for operational efficiency improvements.		
WBPA10	Integration and Governance	The solution shall integrate seamlessly with Enterprise Document & Records Management, Digital Signature Platform, Financial Management, Human Capital & Payroll, Supply Chain & Electronic Procurement, Contract Lifecycle Management, Enterprise Asset Management, Oil Pipeline & Terminal Operations, Customer Self-Service Portal, AI, Analytics & Enterprise Reporting, Identity & Access Management, and other enterprise applications while providing secure APIs, workflow automation, notifications, and comprehensive auditability of all business process automation activities.		

2.2.4.2.9.3 Master Data Governance

The proposed solution shall provide an integrated Master & Reference Data Management capability to establish a single source of truth for enterprise master data and reference data across all business functions. The solution shall support standardized data governance, data quality, lifecycle management, validation, synchronization, and stewardship to ensure consistency, integrity, and accuracy of information across all enterprise applications and integrations.

Functional Requirements

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
MDM01	Master Data Governance	The solution shall support enterprise-wide governance of master data through configurable ownership, stewardship, approval workflows, validation rules,		

Code	Functional Area	Functional Requirements	Tenderers Response (Yes/No)	Evidence Page
		data standards, policies, lifecycle management, and audit controls.		
MDM02	Enterprise Master Data Management	The solution shall support centralized management of master data entities including customers, suppliers, employees, assets, materials, products, services, locations, projects, contracts, chart of accounts, cost centres, business partners, and other enterprise master records.		
MDM03	Reference Data Management	The solution shall support management of reference data including organizational structures, business units, classifications, currencies, units of measure, tax codes, countries, regulatory codes, calendars, and configurable business reference data.		
MDM04	Data Quality and Validation	The solution shall support configurable validation rules, duplicate detection, data cleansing, standardization, completeness checks, exception management, quality scoring, and continuous monitoring of master data quality.		
MDM05	Master Data Lifecycle Management	The solution shall support creation, review, approval, publication, modification, version control, archival, retirement, and restoration of master and reference data throughout its lifecycle.		
MDM06	Data Synchronization and Distribution	The solution shall support automated synchronization, replication, publishing, and distribution of master data across enterprise applications, external systems, APIs, integration platforms, and digital services while maintaining data consistency.		
MDM07	Metadata and Data Lineage Management	The solution shall support management of metadata, business glossaries, data lineage, data relationships, impact analysis, and traceability of master data across enterprise processes and information systems.		
MDM08	Master Data Reporting and Analytics	The solution shall provide configurable dashboards, data quality reports, duplicate analysis, stewardship reports, data completeness metrics, executive dashboards, KPI monitoring, and self-service reporting with drill-down capabilities.		
MDM09	Workflow and Governance	The solution shall support configurable workflows, delegated authority, approvals, notifications, audit trails, segregation of duties, document attachments, and complete traceability of all master data management activities.		
MDM10	Integration and Governance	The solution shall integrate seamlessly with all enterprise applications, databases, integration platforms, business intelligence solutions, identity management services, enterprise document management, and external data sources while providing role-based security, workflow automation, notifications, and comprehensive auditability of all master and reference data management activities.		

2.2.4.2.10 Infrastructure Requirements

This section defines the detailed technical, architectural, operational, security, and resilience requirements for the infrastructure and platform components supporting the proposed Enterprise Digital Transformation Solution. It establishes the minimum standards for deployment, performance, scalability, interoperability, security, availability, business continuity, disaster recovery, manageability, and operational sustainability.

Kenya Pipeline Company PLC (KPC) operates critical national energy infrastructure and is subject to applicable legislation, regulations, standards, and directives governing Critical Information Infrastructure (CII), cybersecurity, data protection, records management, operational resilience, and business continuity. The proposed solution shall therefore be designed and implemented in a manner that safeguards the confidentiality, integrity, availability, sovereignty, and resilience of KPC's critical information assets and operational systems.

The MSOOS and TMS within this project **shall** be deployed on KPC premises while the ERP shall be hosted on KPC premises or in-country cloud. Any cloud deployment shall be compliant with data protection act both for primary and secondary sites with the various data processors clearly disclosed. The deployment strategy for e-Procurement, e-HR and Analytic/AI is cloud first.

The proposed infrastructure shall provide a secure, scalable, highly available, resilient, and future-ready environment capable of supporting virtualized, containerized, cloud-enabled, and hybrid workloads. The architecture shall incorporate high availability, disaster recovery capabilities across primary and disaster recovery sites, automated failover and recovery mechanisms, cybersecurity controls, centralized monitoring and observability, immutable backup capabilities, cyber-recovery mechanisms, performance optimization, automation, and operational intelligence.

All infrastructure components proposed for both the Primary Site and Disaster Recovery Site shall be enterprise-grade, OEM-supported, and designed with no single point of failure. The infrastructure shall support continuous operations of critical business and operational systems and provide sufficient capacity to accommodate future business growth, technology modernization, and evolving operational requirements.

The Contractor shall provide all infrastructure, software, licenses, services, configurations, and supporting components required to deliver a fully operational solution, including but not limited to:

i. Compute infrastructure optimized for enterprise, database, analytics, integration, and distributed workloads;
ii. Virtualization and container orchestration platforms supporting workload mobility, automation, high availability, and dynamic resource allocation;
iii. Software-defined storage platforms supporting scalable, resilient, high-performance storage services;
iv. High-speed, resilient network infrastructure supporting enterprise, storage, backup, disaster recovery, and operational workloads;
v. Enterprise backup, recovery, cyber-recovery, and data immutability platforms supporting ransomware resilience, long-term retention, and rapid restoration of services;
vi. Load balancing, application delivery, traffic management, and workload optimization platforms;
vii. Enterprise monitoring, observability, event management, and AIOps platforms providing end-to-end visibility across infrastructure, platforms, applications, integrations, and services;
viii. Integration, API management, automation, and orchestration platforms supporting interoperability and Infrastructure-as-Code (IaC) practices;

ix. Integration to Identity and Access Management (IAM), Privileged Access Management (PAM), and Zero Trust security infrastructure;
x. Infrastructure automation, configuration management, and lifecycle management platforms;
xi. Disaster recovery, replication, failover, and business continuity platforms; and
xii. Any additional infrastructure, software, services, licenses, tools, or components necessary to provide a complete, secure, resilient, maintainable, and fully integrated solution.

The proposed infrastructure architecture shall:

i. Support high availability and continuous operation of all critical workloads;
ii. Support horizontal and vertical scalability without significant architectural redesign;
iii. Support secure integration and convergence between Information Technology (IT) and Operational Technology (OT) environments;
iv. Support centralized administration, monitoring, observability, automation, and governance;
v. Support automated failover, disaster recovery, and workload recovery capabilities;
vi. Support immutable backups, cyber-recovery, ransomware protection, and rapid restoration of services;
vii. Support future growth, technology modernization, and evolving business requirements;
viii. Support interoperability with existing and future enterprise, operational, cloud, government, and third-party platforms;
ix. Support secure remote administration, auditing, monitoring, and controlled third-party access in accordance with Critical Information Infrastructure requirements;
x. Support Infrastructure-as-Code (IaC), automation, DevSecOps, and modern platform management practices where applicable;
xi. Support compliance with cybersecurity, data protection, records management, Critical Information Infrastructure protection, and applicable regulatory requirements; and
xii. Provide a sustainable, maintainable, vendor-supported platform capable of supporting KPC's long-term digital transformation strategy while ensuring operational resilience and business continuity.
xiii. Support Recovery Time Objectives (RTO) of less than 30Min and Recovery Point Objectives (RPO) of less than 2Hours

2.2.4.2.10.1 Compute and Storage

Compute Platform for Primary Site

The Contractor shall provide, install, configure, test, and commission an enterprise-grade compute platform at the Primary Site and DR Site to host the Corporation's Digital Transformation Platform and all associated business, operational, integration, analytics, and cybersecurity workloads. Its expected that the platforms will be hybrid in nature therefore the resources required by each system should be coupled with the specific system in the hosting platform.

The platform shall provide a secure, highly available, scalable, and resilient computing environment capable of supporting both traditional virtual machine workloads and modern cloud-native applications within a unified management framework.

Core Compute Compliance Matrix for Primary

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
CC01	**Compute Infrastructure**		
1.	The solution shall provide enterprise-grade compute infrastructure designed for mission-critical ERP, database and enterprise business workloads. The architecture shall support virtualization, workload isolation, resource pooling, dynamic resource allocation, high availability, and non-disruptive maintenance operations.		
2.	The solution shall support enterprise operating systems required for business applications, with native OEM-supported lifecycle management, including provisioning, configuration, patching, monitoring, security updates, and system maintenance.		
3.	The solution shall provide built-in redundancy across compute, memory, storage, networking, management, power, cooling, and system interconnect components. No single hardware component failure shall result in loss of service for production workloads.		
4.	The solution shall provide automated fault detection, workload protection, self-healing capabilities, and automated failover mechanisms capable of maintaining service availability during component, node, storage, network, or management failures.		
5.	The solution shall support workload mobility and automated workload restart or migration to available resources in the event of planned or unplanned outages.		
6.	The solution shall support rolling software, firmware, and infrastructure updates with minimal or no disruption to production workloads.		
7.	For every node, the proposed compute platform shall support ECC (Error Correcting Code) memory for protection against memory errors and data corruption. The tenderer shall confirm compliance and provide supporting documentation from the OEM.		
8.	The platform shall support clustered operation of compute resources with centralized management and shared access to workload resources across the environment.		
CC02	**Scalability and Hardware Capacity**		
9.	The architecture shall support both vertical (scale-up) and horizontal (scale-out) expansion while maintaining application availability, management consistency, workload protection, and operational continuity.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
10.	The proposed platform shall provide a minimum effective processing capacity of **688 physical processor cores** for Primary Site, and based on the latest generation x86 processor technology available from the proposed OEM at the time of bid submission. The proposed processors shall have a **minimum base clock frequency of 3.0 GHz**. The minimum required processor capacity shall remain available after accounting for resources reserved for high availability, node failure tolerance, workload failover, and planned maintenance activities. The tenderer shall clearly indicate the processor manufacturer, processor model, processor generation, processor clock frequency, total installed processor capacity, reserved capacity, failover capacity, and available production capacity under both normal operating conditions and single-node failure scenarios.		
11.	The proposed platform shall provide a minimum effective memory capacity of **8192GB RAM**. The minimum required memory capacity shall remain available after accounting for resources reserved for high availability, node failure tolerance, workload failover, and planned maintenance activities. The tenderer shall clearly indicate the total installed memory capacity, reserved capacity, failover capacity, and available production capacity under both normal operating conditions and single-node failure scenarios.		
12.	All installed memory modules shall be Registered DIMMs (RDIMMs) operating at a minimum speed of 6,400 MT/s (6400 MHz) or higher, fully supported by the proposed server architecture and processor configuration.		
13.	The proposed server shall support a minimum of 10 x SFF hot-pluggable internal drive bays per server node. Tenderer shall provide OEM documentation confirming the supported drive configurations.		
14.	The proposed server shall be supplied with 1 x BOSS-N1 controller card (or OEM equivalent) and 2 x 960GB M.2 SSDs (2280 form factor) configured in RAID 1 per server node.		
15.	The proposed server shall be equipped with an enterprise-class hardware RAID controller supporting RAID levels 0, 1, 5, 6, 10, 50, and 60. The controller shall include a minimum of 8 GB battery-backed cache (or OEM-equivalent cache protection technology). OEM documentation shall be provided to confirm compliance.		
16.	The proposed platform shall provide high-performance, low-latency server-to-storage connectivity with a minimum aggregate bandwidth of 64Gbps per server. Solutions based on RDMA-enabled technologies, including NVMe/RDMA (RoCE or equivalent) and NVMe over Fabrics (NVMe-oF), are preferred. Alternative enterprise-grade storage networking technologies may be proposed, provided they meet or exceed the required performance, latency, resiliency, and availability characteristics.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
17.	The proposed server shall support the installation of up to 4 enterprise-class GPUs for future analytics, AI/ML, HPC, and accelerator-based workloads. The tenderer shall provide OEM documentation confirming the maximum supported GPU capacity and associated power and cooling capabilities.		
18.	The proposed server shall provide a minimum of 3 PCIe expansion slots per node based on the latest PCIe generation supported by the platform.		
19.	The proposed server shall be supplied with a minimum of 6 hot-pluggable cooling fans configured to provide redundant cooling and continuous operation in the event of a fan failure.		
20.	The proposed server nodes shall be supplied with dual hot-pluggable 1,500W power supplies, configured in 1+1 redundant mode, supporting 200–240 VAC input power and certified to 80 PLUS Titanium efficiency standards (or equivalent).		
21.	For each node, the proposed server shall be supplied with 1 x dedicated management port**,** at least 3 x USB ports**,** and 1 x VGA port**.** The dedicated management interface shall support secure remote administration, monitoring, diagnostics, and power management.		
22.	The proposed server shall support hot-swappable drives, cooling fans, and power supply units, enabling replacement without requiring system shutdown or disruption to production workloads.		
23.	The proposed server shall provide a Silicon Root of Trust or equivalent hardware-based security technology to protect firmware, BIOS, and critical platform components from unauthorized modification. The solution shall support firmware integrity validation, secure boot, and secure recovery capabilities.		
24.	The proposed Disaster Recovery (DR) platform shall provide a minimum effective processor capacity equivalent to 60% of the effective processor capacity provided at the Primary Site.		
25.	The proposed Disaster Recovery (DR) platform shall provide a minimum effective memory capacity equivalent to 60% of the effective memory capacity provided at the Primary Site.		
26.	The platform shall provide protection for sensitive data in use through hardware-assisted memory protection, memory encryption, confidential computing capabilities, or equivalent vendor-supported technologies designed to protect workload memory from unauthorized access.		
27.	The tenderer shall provide Enterprise Linux server and Windows Server licensing and subscription entitlements sufficient to support the full compute capacity of the proposed platform, including virtual machine and containerized workloads, while maintaining support for high availability, workload mobility, failover, disaster recovery, and planned maintenance operations without additional licensing requirements.		
28.	The platform shall provide a shared resource architecture enabling compute, memory, storage, and networking resources to be logically pooled, managed, and allocated to workloads based on policy and operational requirements.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
29.	The platform shall support non-disruptive, on-demand allocation of compute, memory, and storage resources without requiring application downtime, redesign or significant reconfiguration.		
30.	The proposed architecture shall eliminate single points of failure across compute, storage, networking, management, power, and infrastructure management components.		
CC03	**Virtualization and Cloud-Native Platform**		
31.	The solution shall provide production-grade containerization capabilities, supporting enterprise container orchestration either natively or through tightly integrated platform components.		
32.	The solution shall support the coexistence of traditional virtual machine workloads and cloud-native containerized workloads within a unified management framework, providing consistent networking, security, monitoring, and administration.		
33.	The platform shall support live and non-disruptive migration of workloads between participating infrastructure resources without interruption to running applications, user sessions, or active network connections.		
34.	The platform shall provide enterprise virtualization capabilities as an integrated platform service or through tightly integrated components. The solution shall support high availability, resource scheduling, workload migration, policy-based automation, workload isolation, and centralized management. Licensing models shall be clearly identified by the tenderer.		
35.	The platform shall support advanced Quality of Service (QoS) capabilities to guarantee compute resource availability and enforce workload prioritization during periods of resource contention. Supported mechanisms may include fractional/sub-core resource allocation, strict oversubscription controls, or automated dynamic load balancing across cluster nodes to isolate critical system performance.		
36.	The platform shall provide native support for cloud-native applications, including containers, microservices, Kubernetes orchestration, and related technologies.		
37.	The platform shall support policy-based workload placement, automated balancing of infrastructure resources, and intelligent workload distribution across available resources.		
38.	The platform shall support integrated orchestration of virtualized and containerized workloads through a unified operational model.		
39.	The proposed virtualization platform shall support both traditional external SAN/NAS storage architectures and Hyper-Converged Infrastructure (HCI) deployment models on the same management and hypervisor framework.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
40.	The platform shall permit non-disruptive enablement of software-defined storage (SDS) and HCI capabilities on the existing hypervisor stack without requiring hypervisor replacement, architectural redesign, reinstallation of virtual machine workloads, or deployment of third-party host agents.		
CC04	**High Availability and Resilience**		
41.	The platform shall support Recovery Time Objectives (RTO) of less than 30Min and Recovery Point Objectives (RPO) of less than 2Hours aligned with business criticality requirements.		
42.	The proposed platform shall provide end-to-end high availability across compute, storage, networking, management, and virtualization layers.		
43.	The solution shall support clustered operation of compute resources under centralized management, enabling shared resource utilization, workload mobility, and high availability across participating infrastructure nodes.		
44.	The platform shall automatically detect infrastructure failures and initiate workload recovery procedures without manual intervention.		
45.	The solution shall support workload protection against hardware failures, software failures, operating system failures, storage failures, and network failures.		
46.	The solution shall support deployment across a Primary Site and Disaster Recovery Site.		
47.	The solution shall support replication of workloads, data, configurations and system metadata between sites.		
48.	The solution shall support planned and unplanned failover and failback operations.		
49.	The tenderer shall specify the achievable Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for all business-critical workloads.		
CC05	**Networking and Integration**		
50.	The platform shall provide high-performance, low-latency network connectivity with minimum network speeds of 25Gbps for internal east-west traffic. Support for 40/100Gbps networking is preferred for high-performance enterprise workloads.		
51.	The proposed solution shall come with **all required** transceivers, fiber optic cabling, and connectivity accessories.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
52.	The platform shall support fully redundant networking, including link aggregation, automated path failover, and physical separation of management, control, storage, and application traffic.		
53.	The platform shall support secure network segmentation and workload isolation through industry-standard technologies such as VLANs and VXLANs or equivalent.		
54.	The solution shall support secure hybrid cloud integration with public and private cloud environments using industry-standard interfaces and management tools.		
55.	The platform shall support secure API-driven integration with enterprise automation, orchestration, and infrastructure management platforms.		
CC06	**Operations, Security and Support**		
56.	The solution shall integrate with existing enterprise cybersecurity platforms.		
57.	The platform shall provide comprehensive infrastructure monitoring and observability, including performance monitoring, health monitoring, centralized logging, alerting, capacity analytics, and reporting.		
58.	The platform shall provide centralized firmware, operating system, and platform lifecycle management, supporting rolling updates and patching with minimal or no planned service disruption where supported by the platform architecture.		
59.	The platform shall support disaster recovery integration, including replication, backup integration, automated failover, workload recovery, and business continuity capabilities.		
60.	The tenderer shall provide OEM-backed enterprise hardware and software support for all supplied components for a minimum period of three (3) years, including software updates, firmware updates, technical support, and replacement of faulty hardware components.		
61.	The tenderer shall provide documented evidence that the OEM maintains a local presence, including a parts warehouse/logistics hub and OEM-certified local support engineers, sufficient to fulfill the required Next Business Day (NBD) parts replacement SLA.		
CC06	**Tenderer Technical Proposal Requirements**		
62.	The tenderer shall provide the proposed compute platform architecture, including the topology, deployment model for the Primary and Disaster Recovery Sites.		
63.	The tenderer shall describe the proposed virtualization and container platform architecture, including workload placement, resource management, and high availability design.		
64.	The tenderer shall provide the proposed scalability model, including current capacity, maximum supported capacity, future expansion approach, and technology roadmap.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
65.	The tenderer shall describe the proposed high availability architecture, including redundancy, clustering, workload migration, failover mechanisms, and resilience against component failures.		
66.	The tenderer shall describe the proposed infrastructure management, monitoring, automation, lifecycle management, and operational support approach.		
67.	The tenderer shall describe the proposed integration with enterprise storage, networking, cybersecurity, backup, disaster recovery, monitoring, identity management, and cloud platforms.		
68.	The tenderer shall provide the proposed implementation methodology, migration approach, testing strategy, cutover plan, rollback procedures, and business continuity considerations.		
69.	The tenderer shall specify the infrastructure availability design and demonstrate how the proposed solution achieves continuous service delivery during component failures and planned maintenance activities.		

2.2.4.2.10.2 Compute Platform for Disaster Recovery Site

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
CC01	**Compute Infrastructure**		
1.	The solution shall provide enterprise-grade compute infrastructure designed for mission-critical ERP, database and enterprise business workloads. The architecture shall support virtualization, workload isolation, resource pooling, dynamic resource allocation, high availability, and non-disruptive maintenance operations.		
2.	The solution shall support enterprise operating systems required for business applications, with native OEM-supported lifecycle management, including provisioning, configuration, patching, monitoring, security updates, and system maintenance.		
3.	The solution shall provide built-in redundancy across compute, memory, storage, networking, management, power, cooling, and system interconnect components. No single hardware component failure shall result in loss of service for production workloads.		
4.	The solution shall provide automated fault detection, workload protection, self-healing capabilities, and automated failover mechanisms capable of maintaining service availability during component, node, storage, network, or management failures.		
5.	The solution shall support workload mobility and automated workload restart or migration to available resources in the event of planned or unplanned outages.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
6.	The solution shall support rolling software, firmware, and infrastructure updates with minimal or no disruption to production workloads.		
7.	For every node, the proposed compute platform shall support ECC (Error Correcting Code) memory for protection against memory errors and data corruption. The tenderer shall confirm compliance and provide supporting documentation from the OEM.		
8.	The platform shall support clustered operation of compute resources with centralized management and shared access to workload resources across the environment.		
CC02	**Scalability and Hardware Capacity**		
9.	The architecture shall support both vertical (scale-up) and horizontal (scale-out) expansion while maintaining application availability, management consistency, workload protection, and operational continuity.		
10.	The proposed platform shall provide a minimum effective processing capacity of **412 physical processor cores** for Primary Site, and based on the latest generation x86 processor technology available from the proposed OEM at the time of bid submission. The proposed processors shall have a **minimum base clock frequency of 3.0 GHz**. The minimum required processor capacity shall remain available after accounting for resources reserved for high availability, node failure tolerance, workload failover, and planned maintenance activities. The tenderer shall clearly indicate the processor manufacturer, processor model, processor generation, processor clock frequency, total installed processor capacity, reserved capacity, failover capacity, and available production capacity under both normal operating conditions and single-node failure scenarios.		
11.	The proposed platform shall provide a minimum effective memory capacity of **4915GB RAM**. The minimum required memory capacity shall remain available after accounting for resources reserved for high availability, node failure tolerance, workload failover, and planned maintenance activities. The tenderer shall clearly indicate the total installed memory capacity, reserved capacity, failover capacity, and available production capacity under both normal operating conditions and single-node failure scenarios.		
12.	All installed memory modules shall be Registered DIMMs (RDIMMs) operating at a minimum speed of 6,400 MT/s (6400 MHz) or higher, fully supported by the proposed server architecture and processor configuration.		
13.	The proposed server shall support a minimum of 10 x SFF hot-pluggable internal drive bays per server node. Tenderer shall provide OEM documentation confirming the supported drive configurations.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
14.	The proposed server shall be supplied with 1 x BOSS-N1 controller card (or OEM equivalent) and 2 x 960GB M.2 SSDs (2280 form factor) configured in RAID 1 per server node.		
15.	The proposed server shall be equipped with an enterprise-class hardware RAID controller supporting RAID levels 0, 1, 5, 6, 10, 50, and 60. The controller shall include a minimum of 8 GB battery-backed cache (or OEM-equivalent cache protection technology). OEM documentation shall be provided to confirm compliance.		
16.	The proposed platform shall provide high-performance, low-latency server-to-storage connectivity with a minimum aggregate bandwidth of 64Gbps per server. Solutions based on RDMA-enabled technologies, including NVMe/RDMA (RoCE or equivalent) and NVMe over Fabrics (NVMe-oF), are preferred. Alternative enterprise-grade storage networking technologies may be proposed, provided they meet or exceed the required performance, latency, resiliency, and availability characteristics.		
17.	The proposed server shall support the installation of up to 4 enterprise-class GPUs for future analytics, AI/ML, HPC, and accelerator-based workloads. The tenderer shall provide OEM documentation confirming the maximum supported GPU capacity and associated power and cooling capabilities.		
18.	The proposed server shall provide a minimum of 3 PCIe expansion slots per node based on the latest PCIe generation supported by the platform.		
19.	The proposed server shall be supplied with a minimum of 6 hot-pluggable cooling fans configured to provide redundant cooling and continuous operation in the event of a fan failure.		
20.	The proposed server nodes shall be supplied with dual hot-pluggable 1,500W power supplies, configured in 1+1 redundant mode, supporting 200–240 VAC input power and certified to 80 PLUS Titanium efficiency standards (or equivalent).		
21.	For each node, the proposed server shall be supplied with 1 x dedicated management port**,** at least 3 x USB ports**,** and 1 x VGA port**.** The dedicated management interface shall support secure remote administration, monitoring, diagnostics, and power management.		
22.	The proposed server shall support hot-swappable drives, cooling fans, and power supply units, enabling replacement without requiring system shutdown or disruption to production workloads.		
23.	The proposed server shall provide a Silicon Root of Trust or equivalent hardware-based security technology to protect firmware, BIOS, and critical platform components from unauthorized modification. The solution shall support firmware integrity validation, secure boot, and secure recovery capabilities.		
24.	The proposed Disaster Recovery (DR) platform shall provide a minimum effective processor capacity equivalent to 60% of the effective processor capacity provided at the Primary Site.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
25.	The proposed Disaster Recovery (DR) platform shall provide a minimum effective memory capacity equivalent to 60% of the effective memory capacity provided at the Primary Site.		
26.	The platform shall provide protection for sensitive data in use through hardware-assisted memory protection, memory encryption, confidential computing capabilities, or equivalent vendor-supported technologies designed to protect workload memory from unauthorized access.		
27.	The tenderer shall provide Enterprise Linux server and Windows Server licensing and subscription entitlements sufficient to support the full compute capacity of the proposed platform, including virtual machine and containerized workloads, while maintaining support for high availability, workload mobility, failover, disaster recovery, and planned maintenance operations without additional licensing requirements.		
28.	The platform shall provide a shared resource architecture enabling compute, memory, storage, and networking resources to be logically pooled, managed, and allocated to workloads based on policy and operational requirements.		
29.	The platform shall support non-disruptive, on-demand allocation of compute, memory, and storage resources without requiring application downtime, redesign or significant reconfiguration.		
30.	The proposed architecture shall eliminate single points of failure across compute, storage, networking, management, power, and infrastructure management components.		
CC03	**Virtualization and Cloud-Native Platform**		
31.	The solution shall provide production-grade containerization capabilities, supporting enterprise container orchestration either natively or through tightly integrated platform components.		
32.	The solution shall support the coexistence of traditional virtual machine workloads and cloud-native containerized workloads within a unified management framework, providing consistent networking, security, monitoring, and administration.		
33.	The platform shall support live and non-disruptive migration of workloads between participating infrastructure resources without interruption to running applications, user sessions, or active network connections.		
34.	The platform shall provide enterprise virtualization capabilities as an integrated platform service or through tightly integrated components. The solution shall support high availability, resource scheduling, workload migration, policy-based automation, workload isolation, and centralized management. Licensing models shall be clearly identified by the tenderer.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
35.	The platform shall support advanced Quality of Service (QoS) capabilities to guarantee compute resource availability and enforce workload prioritization during periods of resource contention. Supported mechanisms may include fractional/sub-core resource allocation, strict oversubscription controls, or automated dynamic load balancing across cluster nodes to isolate critical system performance.		
36.	The platform shall provide native support for cloud-native applications, including containers, microservices, Kubernetes orchestration, and related technologies.		
37.	The platform shall support policy-based workload placement, automated balancing of infrastructure resources, and intelligent workload distribution across available resources.		
38.	The platform shall support integrated orchestration of virtualized and containerized workloads through a unified operational model.		
39.	The proposed virtualization platform shall support both traditional external SAN/NAS storage architectures and Hyper-Converged Infrastructure (HCI) deployment models on the same management and hypervisor framework.		
40.	The platform shall permit non-disruptive enablement of software-defined storage (SDS) and HCI capabilities on the existing hypervisor stack without requiring hypervisor replacement, architectural redesign, reinstallation of virtual machine workloads, or deployment of third-party host agents.		
CC04	**High Availability and Resilience**		
41.	The platform shall support Recovery Time Objectives (RTO) of less than 30Min and Recovery Point Objectives (RPO) of less than 2Hours aligned with business criticality requirements.		
42.	The proposed platform shall provide end-to-end high availability across compute, storage, networking, management, and virtualization layers.		
43.	The solution shall support clustered operation of compute resources under centralized management, enabling shared resource utilization, workload mobility, and high availability across participating infrastructure nodes.		
44.	The platform shall automatically detect infrastructure failures and initiate workload recovery procedures without manual intervention.		
45.	The solution shall support workload protection against hardware failures, software failures, operating system failures, storage failures, and network failures.		
46.	The solution shall support deployment across a Primary Site and Disaster Recovery Site.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
47.	The solution shall support replication of workloads, data, configurations and system metadata between sites.		
48.	The solution shall support planned and unplanned failover and failback operations.		
49.	The tenderer shall specify the achievable Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for all business-critical workloads.		
CC05	**Networking and Integration**		
50.	The platform shall provide high-performance, low-latency network connectivity with minimum network speeds of 25Gbps for internal east-west traffic. Support for 40/100Gbps networking is preferred for high-performance enterprise workloads.		
51.	The proposed solution shall come with **all required** transceivers, fiber optic cabling, and connectivity accessories.		
52.	The platform shall support fully redundant networking, including link aggregation, automated path failover, and physical separation of management, control, storage, and application traffic.		
53.	The platform shall support secure network segmentation and workload isolation through industry-standard technologies such as VLANs and VXLANs or equivalent.		
54.	The solution shall support secure hybrid cloud integration with public and private cloud environments using industry-standard interfaces and management tools.		
55.	The platform shall support secure API-driven integration with enterprise automation, orchestration, and infrastructure management platforms.		
CC06	**Operations, Security and Support**		
56.	The solution shall integrate with existing enterprise cybersecurity platforms.		
57.	The platform shall provide comprehensive infrastructure monitoring and observability, including performance monitoring, health monitoring, centralized logging, alerting, capacity analytics, and reporting.		
58.	The platform shall provide centralized firmware, operating system, and platform lifecycle management, supporting rolling updates and patching with minimal or no planned service disruption where supported by the platform architecture.		
59.	The platform shall support disaster recovery integration, including replication, backup integration, automated failover, workload recovery, and business continuity capabilities.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
60.	The tenderer shall provide OEM-backed enterprise hardware and software support for all supplied components for a minimum period of three (3) years, including software updates, firmware updates, technical support, and replacement of faulty hardware components.		
61.	The tenderer shall provide documented evidence that the OEM maintains a local presence, including a parts warehouse/logistics hub and OEM-certified local support engineers, sufficient to fulfill the required Next Business Day (NBD) parts replacement SLA.		
CC06	**Tenderer Technical Proposal Requirements**		
62.	The tenderer shall provide the proposed compute platform architecture, including the topology, deployment model for the Primary and Disaster Recovery Sites.		
63.	The tenderer shall describe the proposed virtualization and container platform architecture, including workload placement, resource management, and high availability design.		
64.	The tenderer shall provide the proposed scalability model, including current capacity, maximum supported capacity, future expansion approach, and technology roadmap.		
65.	The tenderer shall describe the proposed high availability architecture, including redundancy, clustering, workload migration, failover mechanisms, and resilience against component failures.		
66.	The tenderer shall describe the proposed infrastructure management, monitoring, automation, lifecycle management, and operational support approach.		
67.	The tenderer shall describe the proposed integration with enterprise storage, networking, cybersecurity, backup, disaster recovery, monitoring, identity management, and cloud platforms.		
68.	The tenderer shall provide the proposed implementation methodology, migration approach, testing strategy, cutover plan, rollback procedures, and business continuity considerations.		
69.	The tenderer shall specify the infrastructure availability design and demonstrate how the proposed solution achieves continuous service delivery during component failures and planned maintenance activities.		

2.2.4.2.10.3 New Enterprise Storage

The Tenderer shall provide, install, configure, test, and commission an enterprise-grade storage platform to support the Corporation's Digital Transformation Platform across the Primary and Disaster Recovery Sites. **Whereas the storage infrastructure is meant for the various applications/systems the installation shall be on-premise even where a hybrid deployment has been proposed.**

The proposed solution shall provide secure, resilient, high-performance, and scalable storage services capable of supporting enterprise applications, operational systems, databases, analytics

platforms, virtualization platforms, backup services, and long-term archival requirements. The storage platform shall ensure high availability, data integrity, business continuity, and seamless integration with the Corporation's compute, network, cybersecurity, backup, and disaster recovery infrastructure.

The Enterprise Storage Platform shall:

i. provide high-performance storage for mission-critical and latency-sensitive enterprise workloads;
ii. provide resilient and highly available storage services with no single points of failure;
iii. support block, file, and other applicable enterprise storage services through a unified management platform;
iv. provide scalable storage capacity and performance to support future business growth;
v. support enterprise data protection, replication, backup, disaster recovery, and cyber recovery capabilities;
vi. provide centralized monitoring, lifecycle management, automation, and operational visibility;
vii. integrate with enterprise virtualization, containers, database, and cloud platforms; and
viii. provide an OEM-supported storage platform throughout the contract period.

The proposed solution shall comprise:

i. Two (2) All-Flash Storage Systems, comprising one (1) system for the Primary Site and one (1) system for the Disaster Recovery Site.
ii. Extension of existing Two (2) Dell Unity XT 480 Unified Storage Systems, comprising one (1) system for the Primary Site and one (1) system for the Disaster Recovery Site.
iii. Four (4) SAN Switches, comprising two (2) switches deployed in a redundant SAN fabric at the Primary Site and two (2) switches deployed in a redundant SAN fabric at the Disaster Recovery Site.

The Primary and Disaster Recovery storage platforms shall operate as an integrated enterprise storage solution supporting secure data replication, high availability, automated failover, failback, and centralized management across both sites.
The proposed storage solution shall support the Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) defined by the KPC for business continuity and disaster recovery.
Detailed technical requirements are provided in the Compliance Matrix below.

2 No. Unified Enterprise ALL NVME Storage

i. Unified Enterprise All NVMe – Primary Site

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
1.	ALL NVME Unified Storage	NVME Unified Enterprise Storage supporting with SAN and NAS functionalities		
2.	Manufacturer Authorization	The tenderer must provide a Manufacturer Authorization Form specific for this tender		
3.	Storage Brand and Model	The proposed storage manufacturer must be recognized as a leader by Gartner. Please attach Gartner magic quadrant for 2024/2025		
4.	Storage Capacity	i. The storage should come configured with NVMe TLC SSDs and provide a guaranteed Data Reduction (DRR) of up to 5:1, provide the product's capacity sizing		
		ii. The proposed storage shall be All Flash NVMe storage configured with 115TB usable before data reduction. Show your capacity sizing		
5.	End of Life	Should not be End of Life or Support within the next 5 years.		
6.	Architecture	Must support both NAS and SAN and managed using one interface without additional gateway/controller		
7.	Storage Scalability	Storage should scale to at least 22PB effective capacity		
8.	Project Implementation schedule	Provide a detailed project implementation schedule		
9.	Support protocols	Solution must support: - 1) Both Block (FC, iscsi) 2) File (CIFS/SMB/NFS) 3) vVol workloads		
10.	Storage array CPUs cores and clock speed	Should have latest generation of CPUs with a minimum of 64 Intel Cores running at atleast 2.0GHZ		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
11.	Controller Cache	Array must have Dual controllers and each controller must be configured with a minimum of 384GB memory cache i.e. 768GB per array		
12.	Support for Caching	The System should have NVRAM drives to support caching of hot data/peak spikes		
13.	Storage controller and expansion connectivity	The connectivity between controllers and expansion should be 100Gbps RDMA based and not SAS.		
14.	Capacity Density	The storage controller and expansion enclosure should support 24 or more drives in 2U for capacity consolidation.		
15.	Supported Drives	The storage should support NVMe SSDs		
16.	Supported Front-End ports	The storage should support the following front-end ports: 1) FC Ports: 8/16/32 Gbit/s 2) IP Ports: 10/25,100 Gb/s		
17.	Solution Architecture	a) Controllers should work in active-active mode. b) LUNs shall not belong to any controller. c) Service loads shall be balanced among two or more controllers.		
18.	Controller Scalability	The storage should be able to scale to a minimum of 8 controllers that shall be in active-active state with load balancing.		
19.	Data reduction/ Efficiency	The solution must support minimum Guaranteed Data Reduction Rates of 5:1 or better (compression and deduplication and shall be in-line)		
20.	System Upgrade	The proposed storage system shall support non-disruptive upgrades, enabling software and firmware updates without restarting controllers, disrupting storage services, or impacting application availability.		
21.	NVME Architecture	By implementing end-to-end NVMe architecture: i. The frontend should support NVMe over Fibre Channel or RDMA. ii. Backend should support NVMe over RDMA or PCIe		
22.	Configured Front-end host ports	The proposed storage must be configured with a) 8*32 Gb FC b) 8*25Gb/s NIC ports and must be populated with respective SFPs		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
23.	RAID Support	The storage shall support RAID 5 and RAID 6		
24.	Supported number of vVOLS	The proposed storage must have the capability to support at least 9,000 vVOLS		
25.	Snapshot Technology	i. Should support immutable snapshots which can be used to secure the organization from cyber attacks ii. Should support space efficient Point in time snapshots		
26.	Replication	Synchronous/ Metro and asynchronous replications shall be supported and licenses must be included		
27.		The tenderer shall install, configure, synchronize, test, document, and commission replication between the Primary and Disaster Recovery storage arrays.		
28.	Cloud Based Management	1. Cloud monitoring for: a. Proactive health scoring b. performance review and detection of anomalies c. Optimization of performance through redistribution of workloads d. Security configurations assessment e. Capacity Planning 2. Should proactively send notifications and recommendations via email and via mobile app. 3. Cybersecurity and Anomaly detection		
29.	Storage capacity prediction	The proposed storage solution shall allow administrators to view overall and detailed storage capacity usage through an intelligent management platform. The solution shall automatically analyze capacity consumption trends, identify workload growth patterns, apply predictive analytics, and provide forecasted capacity utilization with proactive recommendations and alerts to facilitate efficient capacity planning and resource optimization.		
30.	Disk Risk Prediction	The storage should have a mechanism to predict disk failure in advance and trigger drive replacement		
31.	Futuristic architecture	The storage should support upgrade to next model by controller swap		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
32.	License	Perpetual license includes but not limit to: - 1) SAN and NAS 2) Snapshot 3) Replication 4) Active-active storage controllers 5) Deduplication and compression 6) WORM 7) QoS 8) Thin Provisioning 9) Block/ File/ vVOls 10) VMware VASA 11) Cloud based monitoring and analytics		
33.	SAN switches Integration	Storage and SAN switches must be from the same Original Equipment Manufacturer (OEM) as the Storage to ensure simplified and seamless integration and support		
34.	Direct server connection	The storage shall support connection to servers directly without use of SAN switches using FC connectivity		
35.	Warranty & Support	The solution shall include 3 years 24x7x365 vendor support, software updates, and 4-hour onsite hardware replacement service		
36.	Compliance	The Storage must comply with the following security features 1) Security technical implementation guide (STIG) 2) Federal Information Processing Standard (FIPS 140) NIST Validated security framework		
37.	Obsolesce	The Data Storage **MUST** not be End of Life or Support within the next five (5) years		

ii. Unified Enterprise All NVMe – DR Site

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
1.	ALL NVME Unified Storage	NVME Unified Enterprise Storage supporting with SAN and NAS functionalities		
2.	Manufacturer Authorization	The tenderer must provide a Manufacturer Authorization Form specific for this tender		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
3.	Storage Brand and Model	The proposed storage manufacturer must be recognized as a leader by Gartner. Please attach Gartner magic quadrant for 2024/2025		
4.	Storage Capacity	iii. The storage should come configured with NVMe TLC SSDs and provide a guaranteed Data Reduction (DRR) of up to 5:1, provide the product's capacity sizing		
		iv. The proposed storage shall be All Flash NVMe storage configured with **70TB usable** before data reduction. Show your capacity sizing		
5.	End of Life	Should not be End of Life or Support within the next 5 years.		
6.	Architecture	Must support both NAS and SAN and managed using one interface without additional gateway/controller		
7.	Storage Scalability	Storage should scale to at least 22PB effective capacity		
8.	Project Implementation schedule	Provide a detailed project implementation schedule		
9.	Support protocols	Solution must support: - 4) Both Block (FC, iscsi) 5) File (CIFS/SMB/NFS) 6) vVol workloads		
10.	Storage array CPUs cores and clock speed	Should have latest generation of CPUs with a minimum of 64 Intel Cores running at least 2.0GHZ		
11.	Controller Cache	Array must have Dual controllers, and each controller must be configured with a minimum of 384GB memory cache i.e. 768GB per array		
12.	Support for Caching	The System should have NVRAM drives to support caching of hot data/peak spikes		
13.	Storage controller and expansion connectivity	The connectivity between controllers and expansion should be 100Gbps RDMA based and not SAS.		
14.	Capacity Density	The storage controller and expansion enclosure should support 24 or more drives in 2U for capacity consolidation.		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
15.	Supported Drives	The storage should support NVMe SSDs		
16.	Supported Front-End ports	The storage should support the following front-end ports: 3) FC Ports: 8/16/32 Gbit/s 4) IP Ports: 10/25,100 Gb/s		
17.	Solution Architecture	d) Controllers should work in active-active mode. e) LUNs shall not belong to any controller. f) Service loads shall be balanced among two or more controllers.		
18.	Controller Scalability	The storage should be able to scale to a minimum of 8 controllers that shall be in active-active state with load balancing.		
19.	Data reduction/ Efficiency	The solution must support minimum Guaranteed Data Reduction Rates of 5:1 or better (compression and deduplication and shall be in-line)		
20.	System Upgrade	The proposed storage system shall support non-disruptive upgrades, enabling software and firmware updates without restarting controllers, disrupting storage services, or impacting application availability.		
21.	NVME Architecture	By implementing end-to-end NVMe architecture: iii. The frontend should support NVMe over Fibre Channel or RDMA. iv. Backend should support NVMe over RDMA or PCIe		
22.	Configured Front-end host ports	The proposed storage must be configured with c) 8*32 Gb FC d) 8*25Gb/s NIC ports and must be populated with respective SFPs		
23.	RAID Support	The storage shall support RAID 5 and RAID 6		
24.	Supported number of vVOLS	The proposed storage must have the capability to support at least 9,000 vVOLS		
25.	Snapshot Technology	iii. Should support immutable snapshots which can be used to secure the organization from cyber attacks iv. Should support space efficient Point in time snapshots		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
26.	Replication	Synchronous/ Metro and asynchronous replications shall be supported and licenses must be included		
27.		The tenderer shall install, configure, synchronize, test, document, and commission replication between the Primary and Disaster Recovery storage arrays.		
28.	Cloud Based Management	4. Cloud monitoring for: a. Proactive health scoring b. performance review and detection of anomalies c. Optimization of performance through redistribution of workloads d. Security configurations assessment e. Capacity Planning 5. Should proactively send notifications and recommendations via email and via mobile app. 6. Cybersecurity and Anomaly detection		
29.	Storage capacity prediction	The proposed storage solution shall allow administrators to view overall and detailed storage capacity usage through an intelligent management platform. The solution shall automatically analyze capacity consumption trends, identify workload growth patterns, apply predictive analytics, and provide forecasted capacity utilization with proactive recommendations and alerts to facilitate efficient capacity planning and resource optimization.		
30.	Disk Risk Prediction	The storage should have a mechanism to predict disk failure in advance and trigger drive replacement		
31.	Futuristic architecture	The storage should support upgrade to next model by controller swap		
32.	License	Perpetual license includes but not limit to: - 12) SAN and NAS 13) Snapshot 14) Replication 15) Active-active storage controllers 16) Deduplication and compression 17) WORM 18) QoS 19) Thin Provisioning 20) Block/ File/ vVOls 21) VMware VASA		

Item no.	Minimum Requirements	Tenderer requirement	Tenderers Response (Yes/No)	Evidence Page
		22) Cloud based monitoring and analytics		
33.	SAN switches Integration	Storage and SAN switches must be from the same Original Equipment Manufacturer (OEM) as the Storage to ensure simplified and seamless integration and support		
34.	Direct server connection	The storage shall support connection to servers directly without use of SAN switches using FC connectivity		
35.	Warranty & Support	The solution shall include 3 years 24x7x365 vendor support, software updates, and 4-hour onsite hardware replacement service		
36.	Compliance	The Storage must comply with the following security features 3) Security technical implementation guide (STIG) 4) Federal Information Processing Standard (FIPS 140) NIST Validated security framework		
37.	Obsolesce	The Data Storage **MUST** not be End of Life or Support within the next five (5) years		

2.2.4.2.10.4 Unified Data Storage Expansion for Existing Dell EMC Unity XT 480 Storage Arrays (2 No.)

Background: KPC currently operates a Dell EMC Unity XT 480 Storage Array. The objective of this procurement is to expand the existing storage infrastructure and not to replace it. The proposed solution must be fully compatible with and supported on the existing Dell EMC Unity XT 480 platform. Tenderers shall provide manufacturer confirmation that the proposed hardware, software, licenses, and drive configurations are supported for integration and operation within the existing storage environment.

Details of the existing Dell EMC Unity XT 480 arrays:

Location	Serial Number	Firmware	Disk Type	Capacity (TB)	Disk Size	RAID
Primary DC	CRK00231108759	5.4.0.0.5.094	SSD	40	19 No. 3.2 TB Flash	RAID 5
Primary DC			SAS	150	121 No. 1.8 TB 10K SAS	RAID 5
Primary DC			NL-SAS	150	42 No. 6 TB 7.2K SATA	RAID 6
DR	CRK00231108722	5.4.0.0.5.094	NL-SAS	120	34 No. 6 TB 7.2K SATA	RAID 6

All expansion shall use original equipment manufacturer (OEM) components. The Tenderer shall disregard the existing disk-array enclosures and provide new enclosures and accessories sufficient

for all proposed disks and shall submit sizing documentation showing the proposed capacity by tier for the primary and DR arrays.
The OEM support renewal for the existing Unity XT 480 arrays (three years) is being procured by KPC PLC separately and will be in place before implementation of this project; it is not part of this tender.

The proposed expansion shall preserve all existing functionality, licenses, performance characteristics, connectivity, and support entitlements of the current storage environment.

	Feature	KPC's Minimum Requirement (Attach datasheet for the proposed solution)	Tenderers Response (Yes/No)	Evidence Page
1.	Make\ Model	The proposed solution shall be a Dell EMC Unity XT-compatible storage expansion and shall be fully supported by the OEM for integration with KPC's existing Dell EMC Unity XT 480 storage array. The tenderer shall provide OEM documentation confirming compatibility and supportability.		
2.	OEM Qualification	The OEM shall have been recognized as a Leader in Gartner Magic Quadrant for Primary Storage for the last three (3) consecutive years. Tenderer shall attach Gartner Magic Quadrant reports for 2023, 2024, and 2025.		
3.	Architecture	The proposed solution shall be a unified hybrid storage platform or expansion component fully compatible with the existing Dell EMC Unity XT 480 storage array, supporting a mix of SSD and HDD drives within the same storage system.		
4.	Form Factor	Where controller hardware is proposed, it shall be supplied in a minimum 2U form factor. For expansion shelves, the proposed form factor shall be fully compatible with the existing Dell EMC Unity XT 480 storage system.		
5.	Maximum Drives	The proposed solution shall support future expansion to the maximum drive count supported by the Dell EMC Unity XT 480 platform without requiring replacement of existing controllers.		
6.	Capacity Required	The proposed expansion shall provide the following additional usable capacity per storage array: **a) Primary Site** i. 20TB SSD storage configured in RAID 5. ii. 50TB SAS storage configured in RAID 6. iii. 100TB NL-SAS storage configured in RAID 6. **b) DR Site** i. 50TB SAS storage configured in RAID 6. ii. 50TB NL-SAS storage configured in RAID 6. The proposed drives shall be fully supported for use within the existing Dell EMC Unity XT 480 storage system. The tenderer shall provide detailed drive sizing calculations showing raw capacity, RAID overhead,		

	Feature	KPC's Minimum Requirement (Attach datasheet for the proposed solution)	Tenderers Response (Yes/No)	Evidence Page
		hot spare allocation (if applicable), and resulting usable capacity.		
7.	Host Connectivity	The proposed expansion shall maintain full compatibility with the existing host connectivity infrastructure and shall not reduce the currently available connectivity capabilities of the existing Dell EMC Unity XT 480 storage array. Where additional front-end connectivity modules, transceivers, or interfaces are required to support the proposed expansion, the tenderer shall provide all necessary components and licenses.		
8.	Availability features	The proposed solution shall support: 1. RAID 5, RAID 6, and RAID 10. 2. Redundant hot-swappable power supplies and cooling fans. 3. No Single Point of Failure (NSPOF) architecture, including controllers, cache, power supplies, fans, storage processors, and connectivity modules. 4. Online, non-disruptive expansion of storage capacity.		
9.	Other features	The proposed storage solution shall support: 1. Inline deduplication, compression, and thin provisioning. 2. Simultaneous support for deduplicated and non-deduplicated volumes. 3. Simultaneous support for compressed and non-compressed volumes. 4. Space-efficient snapshots and thin clones. 5. Immutable snapshots for cyber-resilience and ransomware protection.		
10.	Remote Replication	The proposed storage solution shall support: 1. Synchronous and asynchronous replication between primary and secondary sites. 2. Replication of incremental changes only. 3. Multiple concurrent snapshot, clone, and replication sessions without significant performance degradation. 4. Replication compatibility with the existing Dell EMC Unity XT storage environment.		
11.	Licenses	The tenderer shall provide all licenses required for the proposed expansion and ensure compatibility with the existing Dell EMC Unity XT 480 storage array, including but not limited to: a) Snapshots b) Thin Clones c) Remote Replication d) QoS e) Storage Management f) Performance Monitoring		

	Feature	KPC's Minimum Requirement (Attach datasheet for the proposed solution)	Tenderers Response (Yes/No)	Evidence Page
		g) Data Reduction Features Licenses shall support the full installed capacity following expansion.		
12.	Host Operating System Support	The Data Storage should support the following Operating System: - 1) Citrix XenServer 2) HPE UX 3) IBM AIX 4) Microsoft Windows Server, including Microsoft HyperV 5) Open VMS 6) Oracle Linux (UEK and RHEL compatible kernels) 7) Oracle Solaris 8) Red Hat Enterprise Linux 9) Red Hat Enterprise Virtualization 10) SUSE Linux Enterprise 11) VMware vSphere 12) Nutanix AHV		
13.	Non-Disruptive Expansion	The proposed expansion shall be installed and integrated into the existing Dell EMC Unity XT 480 storage array without requiring data migration, application downtime, host reconfiguration, or disruption to production services. Capacity additions shall be performed online and non-disruptively.		
14.	Obsolescence	The proposed hardware and software shall **NOT** be End-of-Sale, End-of-Life, or End-of-Support within five (5) years from the date of delivery.		
15.	Warranty and Support	1) The OEM must show proof of local presence with parts warehouse/hub and local support engineers to fulfill the Same business day parts replacement SLA with a 4hr response time 2) A minimum of three (3) years Hardware\Software warranty on the product		
16.	Compatibility Certification	Upon completion, the tenderer shall provide OEM-supported documentation confirming that the expansion has been successfully installed and integrated into the existing Dell EMC Unity XT 480 storage array and is fully supported by the OEM.		

2.2.4.2.10.5 SAN Switches

4 No. SAN Switches

No	Item	Minimum Requirements	Tenderers Response (Yes/No)	Evidence Page
1.	Switch Model	Proposed SAN switches should have 64 physical ports supporting minimum 64 Gbps connectivity.		

No	Item	Minimum Requirements	Tenderers Response (Yes/No)	Evidence Page
2.	Fiber channel ports	The switch shall support 64 non-blocking Fibre Channel ports, delivering high port density in a 1U form factor and enabling scalable storage networking deployments.		
3.	Active ports	The solution shall include: i. Minimum 32 activated Fibre Channel ports ii. 32 x 64Gbps Fibre Channel SFPs/transceivers iii. 5 x 3m OM4 LC-LC Duplex Fibre Patch Cords iv. Additional ports shall be licensable without hardware replacement. All activated ports shall be factory-installed, licensed, and fully operational upon commissioning		
4.	Port Scalability	Switch shall support incremental port activation licensing up to full 64 ports.		
5.	Advanced port features	The SAN switch shall support: i. Virtual SAN/Fabric segmentation (VSAN or equivalent) ii. Inter-VSAN Routing (IVR) or equivalent iii. Port Channel/ISL Trunking iv. Multipath load balancing v. Flow-based QoS vi. Zone-based QoS vii. NPIV support		
6.	Performance	Each port shall support auto-negotiation and operation at 16 Gbps, 32 Gbps, and 64 Gbps speeds.		
7.	Credit Loss Recovery	The proposed SAN switches shall provide credit loss recovery and congestion management capabilities to detect, isolate, and recover from buffer credit loss conditions without fabric disruption.		
8.	Clear Link Diagnostics	The proposed SAN switches must include ClearLink Diagnostics (or equivalent functionality) that enables pre-deployment validation and continuous monitoring of Fibre Channel links and support of high-performance fabrics.		
9.	Aggregate bandwidth	The switch shall provide a minimum aggregate switching bandwidth of 4 Tbps full duplex.		
10	Port types	The SAN switch shall support industry-standard Fibre Channel port types including: i. F-Port ii. E-Port iii. EX-Port iv. Diagnostic Port (D-Port or equivalent) v. AE_Port(or equivalent vendor-specific trunking/aggregation port type)		

No	Item	Minimum Requirements	Tenderers Response (Yes/No)	Evidence Page
11	Management	The SAN switch shall integrate with a centralized management platform providing: i. Cloud-based or on-premises management ii. Health monitoring iii. Performance analytics iv. Capacity planning v. Alerting and reporting vi. Automated configuration backup		
12	SAN Switches Integration	The SAN switch solution shall be supplied by the same manufacturer as the proposed storage solution to ensure end-to-end compatibility, interoperability and firmware alignment.		
13	Rack Mounting	The switch shall be supplied with rack mounting rails, brackets, and all accessories required for installation in a standard 19-inch rack.		
14	Hardware Redundancy	The SAN switch shall be equipped with dual hot-swappable redundant power supplies and redundant hot-swappable fan modules. The switch shall be designed with no single point of failure and shall support continuous operation in the event of a power supply or fan module failure.		
15	Non-Disruptive Upgrades	The solution shall support non-disruptive firmware upgrades and maintenance operations wherever applicable.		
16	Indicators	The switch shall provide visual LED indicators for system health, port status, link activity, fan modules, and power supplies.		
17	Standards-Based Interoperability	The SAN switch shall comply with current Fibre Channel industry standards and support interoperability with standards-compliant Fibre Channel switches, storage systems, host bus adapters (HBAs), servers, storage systems and SAN infrastructures from multiple vendors.		
18	Audit Logging	The solution shall maintain detailed audit logs of configuration changes, access attempts, and administrative activities.		
19	Centralized Management	The SAN switches shall be managed through a centralized management platform supporting all deployed switches.		
20	Performance Monitoring	The solution shall provide real-time monitoring of port utilization, throughput, latency, congestion events, errors, and link health.		
21	Software Licensing	Include all licenses required for activated ports, trunking, diagnostics, fabric management, monitoring and analytics.		
22	Health Monitoring	The solution shall continuously monitor switch hardware, power supplies, fan modules and optics		
23	Automated Backup	The solution shall Support automated backup and restoration of switch configurations.		

No	Item	Minimum Requirements	Tenderers Response (Yes/No)	Evidence Page
24	Training	The tenderer shall provide comprehensive instructor-led Administration, Operation, Maintenance, Troubleshooting, Monitoring, and Security training for a minimum of five (5) technical staff. The training shall include both theoretical and hands-on practical sessions		
25	Warranty & Support	The solution shall include 3 years 24x7x365 OEM support, software & firmware updates, and 4-hour onsite hardware replacement service		

2.2.4.2.10.6 Cloud Automation and Orchestration Platform

KPC requires a centralized Cloud Automation and Orchestration Platform to provide unified management, automation, monitoring, and lifecycle administration of the proposed server, Storage, SAN, and associated infrastructure components. The platform shall enable the efficient provisioning, configuration, monitoring, maintenance, and optimization of the infrastructure environment through a single management interface, while supporting vendor best practices for security, availability, scalability, and operational efficiency.

Cloud Automation and Orchestration Platform Requirements

Item no.	Minimum requirements	Tenderer requirement compliance (yes/no)	Evidence page
1.	The tenderer shall provide an Automation Platform for centralized orchestration, automation, and lifecycle management of the proposed infrastructure environment, covering servers, storage, SAN, and network-connected infrastructure components.		
2.	The platform shall include all licenses, subscriptions, agents, connectors, and software components required to centrally discover, monitor, provision, automate, and manage the full lifecycle of all proposed servers, storage systems, SAN, network infrastructure, and other related components.		
3.	The solution shall provide centralized provisioning, configuration, compliance monitoring, firmware/driver lifecycle orchestration, and operational automation from a unified management interface.		
4.	The platform shall support role-based access control, secure authentication, and audit logging for all administrative activities.		
5.	The solution shall support integration with enterprise authentication services such as Active Directory and/or LDAP.		
6.	The platform shall support secure communications using HTTPS/TLS and certificate-based trust for managed infrastructure endpoints.		
7.	The solution shall support automated discovery and inventory of managed infrastructure assets including compute, storage, and fabric elements where applicable.		
8.	The platform shall provide template-based deployment and policy-driven configuration for repeatable infrastructure provisioning.		
9.	The solution shall support at least three automation workflows covering Day 0 initial deployment, Day 1 expansion, and Day 2		

Item no.	Minimum requirements	Tenderer requirement compliance (yes/no)	Evidence page
	operational maintenance activities and configuration drift remediation.		
10	The platform shall support firmware, BIOS, driver, and systems management updates through orchestrated, policy-based lifecycle workflows with minimal operational disruption.		
11	The solution shall provide health monitoring, alerting, reporting, and operational dashboards for managed infrastructure.		
12	The platform shall provide predictive analytics for infrastructure health, capacity forecasting, anomaly detection, and performance optimization recommendations.		
13	The solution shall support integration with IT service management and/or automation ecosystems through standard APIs such as REST API.		
14	The platform shall support integration with common automation frameworks such as Ansible, Terraform, VMware, or equivalent ecosystem tools where applicable to the proposed architecture.		
15	The solution shall support event-driven automation and the execution of scripted or policy-based remediation actions for common infrastructure incidents.		
16	The platform shall support backup and restore of its configuration and automation policies.		
17	The platform shall provide multi-admin management capability with granular permissions for operations, security, and audit teams.		
18	The tenderer shall include architecture design, installation, configuration, integration, knowledge transfer, and documentation for the Automation Platform.		
19	The tenderer shall provide a detailed implementation plan showing platform deployment, discovery, policy creation, onboarding of managed assets, testing, and handover.		
20	The platform shall provide interoperable, unified management of the proposed Server, Storage, SAN, and related infrastructure environment without requiring additional software purchases, and the tenderer shall document such interoperability in the submitted solution design.		
21	The solution shall include vendor best-practice security hardening guidance and recommended operational baseline configuration.		
22	The solution shall include a minimum of 3 years of software support, updates, and 24x7 remote technical support.		
23	The tenderer shall specify the maximum supported number of managed servers, storage systems, SAN switches, and managed devices without additional platform redesign.		

2.2.4.2.10.7 Database and High Availability Infrastructure

The Contractor shall provide, install, configure, test, and commission an enterprise-grade Database and High Availability Platform to support resilient, secure, high-performance, and continuously available databases for the Corporation's Digital Transformation Platform.

The proposed solution shall provide database clustering, replication, failover, workload balancing, connection management, disaster recovery, monitoring, automation, and secure database across the Corporation's enterprise compute, storage, and network infrastructure.

The solution should support high availability, business continuity, operational resilience, and future scalability using industry-standard enterprise compute platforms, certified virtualization layers, or vendor-validated hardware architecture tailored to the specific workload requirements.

The Database and High Availability Platform shall:

1. provide resilient, highly available database through native or platform-assisted clustering, synchronous and asynchronous replication, automated failover, and workload balancing;
2. support secure database, connection management, workload routing, and database resilience across Primary and Disaster Recovery Sites;
3. support high-performance transactional processing, analytical workloads, and modern database deployment models on certified enterprise infrastructure;
4. provide centralized monitoring, automation, lifecycle management, performance optimisation, backup, recovery, and operational visibility;
5. support disaster recovery, business continuity, data protection, and automated recovery orchestration aligned with enterprise Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs);
6. support enterprise relational database engines, specialized in-memory data platforms, multi-model capabilities, and cloud-native database architectures as required by the hosted enterprise applications;
7. integrate seamlessly with enterprise applications, integration platforms, analytics platforms, monitoring solutions, cybersecurity platforms, and cloud environments; and
8. provide an OEM-supported Database and High Availability Platform throughout the contract period.

The proposed solution shall include all software, licences, clustering services, replication services, failover services, management components, monitoring capabilities, implementation services, training, and supporting infrastructure required to deliver a fully integrated Database and High Availability Platform operating on the Corporation's enterprise infrastructure.

Detailed technical requirements are provided in the Database and High Availability Services Compliance Matrix below.

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
DAHA01	**Platform Foundation & High Availability**		
1	The platform shall support deployment on shared enterprise compute, storage, and network infrastructure, including physical, virtualized, vendor-validated engineered systems, containerized, cloud, and hybrid environments.		
2	The platform shall provide high availability capabilities including native or platform-assisted clustering, replication, automatic failover, failback, workload balancing, and connection routing.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
3	The platform shall support active-active and active-passive deployment architectures across multiple nodes and sites.		
4	The platform shall support synchronous and asynchronous replication, quorum management, split-brain prevention, and automated role assignment.		
5	The platform shall provide ACID-compliant transaction processing with high performance, scalability, and reliability for enterprise relational and in-memory workloads.		
6	The platform shall support horizontal and vertical scalability, including partitioning, scale-up/scale-out architectures, storage management, and elastic capacity expansion.		
7	The platform shall support multi-site, multi-datacenter, and multi-region deployment, disaster recovery, point-in-time recovery, backup, restoration, and automated recovery orchestration across on-premises, hybrid, and cloud environments.		
DAHA02	**Security, Data Protection & Database Services**		
8	The platform shall support encryption of data at rest and in transit, role-based access controls, auditing, masking, data protection, and compliance management capabilities.		
9	The platform shall support logical isolation, workload management, resource governance, and multi-tenancy capabilities where applicable.		
10	The platform shall support integration with enterprise applications, APIs, streaming platforms, ETL/ELT tools, batch processing systems, and data ingestion platforms.		
11	The platform shall support real-time and log-based replication, data synchronization, and Change Data Capture (CDC) capabilities.		
12	The platform shall provide advanced query optimization, indexing, caching, in-memory processing, workload analysis, and performance tuning capabilities.		
13	The platform shall support transactional processing, analytical workloads, reporting, and integration with Business Intelligence and analytics platforms.		
14	The platform shall support automated provisioning, patch management, upgrades, tuning, monitoring, anomaly detection, and operational automation.		
15	The platform shall provide comprehensive monitoring, performance management, audit logging, transaction logging, and integration with enterprise monitoring and SIEM platforms.		
16	The platform shall support full, incremental, differential, storage snapshot, and point-in-time backup and recovery capabilities.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
17	The platform shall support online schema changes, rolling upgrades, zero or near-zero downtime maintenance, and configuration changes with minimal disruption to business operations.		
18	The platform shall provide standard SQL, native enterprise application client adapters, REST, API-based, and programmatic access interfaces for application and integration development.		
DAHA03	**Modern Database & AI Capabilities**		
19	The platform shall support deployment across on-premises data centers, vendor-validated engineered systems, private cloud and hybrid environments.		
20	The platform shall support enterprise virtualization platforms, bare-metal deployments, container orchestration environments, and cloud-native deployment models.		
21	The platform shall support in-memory processing, advanced caching, columnar/row compression, data tiering, archiving, and retention management capabilities.		
22	The platform shall provide centralized administration through graphical, command-line, web-based consoles, and API-based management interfaces.		
23	The platform shall support integration with load balancers, DNS services, virtual IPs, cluster managers, service discovery platforms, and disaster recovery orchestration solutions.		
24	The platform shall support multi-model capabilities including relational, document, JSON, spatial, graph, time-series, or specialized in-memory data structures where applicable to the underlying database engine.		
25	The platform shall support AI-ready capabilities including vector data types, embeddings, similarity search, AI-assisted query optimization, or native integrations with enterprise machine learning platforms where applicable.		
26	The platform shall support machine learning model integration, scoring, inference, lifecycle management, and AI-driven workload optimization capabilities where supported by the database engine architecture.		
27	The platform shall support metadata management, data lineage, policy enforcement, data governance, and comprehensive auditability capabilities.		
DAHA04	**Tenderer Technical Proposal Requirements**		
28	The tenderer shall provide the proposed Database and High Availability architecture, including topology diagrams, component sizing, and failover workflows across Primary and Disaster Recovery Sites.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
29	The tenderer shall provide the sizing methodology, assumptions, and calculations used to determine the proposed compute, memory, IOPS/storage bandwidth, networking, clustering, and database capacities for all hosted enterprise workloads.		
30	The tenderer shall describe the proposed database architecture, including native and platform-assisted clustering, replication (synchronous/asynchronous), failover, workload balancing, backup, disaster recovery orchestration, and business continuity approach across Primary and Secondary sites.		
31	The tenderer shall describe the proposed scalability model (scale-up and scale-out), throughput and memory/IOPS characteristics, high availability architecture, failover and failback behavior, RPO/RTO targets, and performance optimization strategy.		
32	The tenderer shall describe the proposed database security, encryption, governance, auditing, centralized monitoring, patch management, operational automation, and lifecycle management approach.		
33	The tenderer shall describe the proposed integration approach with enterprise applications, integration platforms, analytics systems, on-premises/cloud services, enterprise monitoring tools, and cybersecurity solutions.		
34	The tenderer shall provide the proposed implementation methodology, database migration approach (including near-zero downtime cutover strategies), testing framework, rollback procedures, knowledge transfer, and operational transition plan.		

2.2.4.2.10.8 Disaster Recovery Requirements

The Contractor shall provide, install, configure, test, and commission an enterprise-grade Disaster Recovery (DR) Compute Platform to support business continuity and disaster recovery for the Corporation's Digital Transformation Platform. Any disaster recovery sites hosted on cloud should comply with Data Protection Act of 2019. The set High Availability requirements apply to both on-premise and on-cloud deployments.

The Disaster Recovery Platform shall provide a secure, resilient, and highly available recovery environment capable of protecting critical business, operational, integration, analytics, and cybersecurity workloads against planned and unplanned disruptions.

The proposed solution shall support automated replication, failover, failback, and recovery orchestration between the Primary Site and the Disaster Recovery Site, ensuring that Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are achieved in accordance with business criticality.

The Disaster Recovery Platform shall:

i. provide a resilient secondary compute environment capable of recovering critical business services during disaster events;
ii. support automated replication, failover, failback, and recovery orchestration for enterprise workloads;
iii. provide application-consistent recovery with appropriate data protection mechanisms based on workload criticality;

iv. support scalable disaster recovery infrastructure aligned with the growth of the primary production environment;
v. provide centralized monitoring, management, reporting, testing, and recovery readiness capabilities;
vi. integrate with enterprise backup, cybersecurity, monitoring, networking, storage, and business continuity platforms;
vii. support secure connectivity, workload isolation, cyber recovery, and regulatory compliance; and
viii. provide an OEM-supported disaster recovery compute platform that enables periodic testing, maintenance, and continuous operational readiness throughout the contract period.

Disaster Recovery Compliance Matrix

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
DR01	**Disaster Recovery Architecture & Availability**		
1	The platform shall support seamless failover of critical business, operational, and technology workloads with minimal disruption to business operations.		
2	The platform shall provide automated failover, failback, recovery orchestration, and recovery workflow management capabilities.		
3	The platform shall support application-consistent and transaction-consistent recovery across multi-tier and distributed workloads.		
4	The platform shall support synchronous, asynchronous, continuous, and policy-based replication mechanisms based on workload criticality and recovery objectives.		
5	The platform shall support regular, automated, and non-disruptive disaster recovery testing, validation, and recovery readiness assessments.		
6	The DR environment shall provide highly available and resilient compute infrastructure with no single points of failure.		
7	The platform shall support Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) aligned with business criticality requirements.		
8	The platform shall support near real-time recovery capabilities for mission-critical applications and services.		
DR02	**Recovery Management & Operations**		
9	The platform shall provide centralized monitoring, management, orchestration, reporting, and operational visibility across DR services.		
10	The solution shall support prioritized, dependency-aware, and staged recovery of business services and applications during disaster events.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
11	The solution shall ensure data integrity, consistency, validation, and reconciliation during replication, failover, and recovery operations.		
12	The platform shall provide audit trails, recovery reporting, compliance reporting, and recovery testing reports.		
13	The platform shall support non-disruptive maintenance, upgrades, testing, and expansion activities.		
DR03	**Infrastructure, Connectivity & Scalability**		
14	The DR platform shall support scalability and expansion in line with growth of production workloads and future business requirements.		
15	The platform shall support heterogeneous operating systems, databases, applications, virtualization platforms, cloud platforms, and containerized workloads.		
17	The platform shall optimize resource utilization and support cost-efficient operation of standby, warm disaster recovery environments.		
18	The platform shall support private cloud, hybrid cloud, virtualized, physical, and containerized deployment models.		
19	The platform shall support automated provisioning, orchestration, Infrastructure-as-Code (IaC), and integration with enterprise automation platforms.		
DR04	**Security, Compliance & Business Continuity**		
20	The DR environment shall support secure workload isolation, segmentation, access controls, and cyber recovery capabilities.		
21	The platform shall support compliance with applicable business continuity, disaster recovery, cybersecurity, and regulatory requirements.		
22	The platform shall integrate with enterprise backup, recovery, cyber recovery, archive, storage, monitoring, and business continuity solutions.		
23	The platform shall support cyber recovery, immutable recovery environments, ransomware recovery, and isolated recovery capabilities.		
DR05	**Tenderer Technical Proposal Requirements**		
24	The tenderer shall provide the proposed Disaster Recovery architecture, including the deployment model for the Primary and Disaster Recovery Sites.		
25	The tenderer shall describe the proposed replication architecture, including replication technologies, replication modes, workload protection strategy, and dependency management.		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
26	The tenderer shall specify the supported Recovery Point Objectives (RPOs), Recovery Time Objectives (RTOs), recovery capacities, and failover/failback times for the proposed solution.		
27	The tenderer shall provide the disaster recovery sizing methodology, assumptions, standby resource allocation, and capacity planning approach for the proposed environment.		
28	The tenderer shall describe the proposed disaster recovery orchestration, automation, testing methodology, recovery validation, and operational readiness approach.		
29	The tenderer shall describe the proposed cyber recovery capabilities, ransomware recovery approach, immutable recovery architecture, and integration with enterprise backup and cybersecurity platforms.		
30	The tenderer shall describe the proposed disaster recovery monitoring, reporting, compliance, and operational management approach.		
31	The tenderer shall provide the proposed implementation methodology, disaster recovery testing approach, migration activities, operational transition plan, and business continuity considerations.		

2.2.4.2.10.9 Load Balancers/Application Delivery Controllers

The tenderer shall provide, install, configure, test, and commission an enterprise-grade Load Balancing Platform to provide intelligent application delivery, secure traffic management, workload distribution, and high availability for the Corporation's Digital Transformation Platform. The proposed solution shall provide resilient, secure, scalable, and centrally managed application delivery services for enterprise applications, web services, APIs, microservices, cloud-native workloads, and business-critical systems deployed across the Primary and Disaster Recovery Sites. The platform shall optimize application availability, performance, security, and user experience while supporting business continuity and future growth.

The Load Balancing Platform shall:

i. provide intelligent Layer 4 and Layer 7 application delivery and traffic management for enterprise workloads;
ii. support high availability, redundancy, automated failover, and resilient application delivery services;
iii. provide secure application delivery through SSL/TLS services, authentication, access controls, and integration with enterprise cybersecurity platforms;
iv. support application acceleration, traffic optimization, caching, compression, and advanced traffic management capabilities;
v. provide centralized administration, monitoring, reporting, analytics, automation, and operational visibility across the application delivery environment;
vi. support hybrid cloud, virtualized, containerized, and cloud-native application deployments;
vii. support scalable, API-driven, and software-defined application delivery architectures that accommodate future business growth; and

viii. provide an OEM-supported Application Delivery Controller (ADC) platform throughout the contract period.

The proposed solution shall include four (4) enterprise Application Delivery Controllers (ADCs), all required software licences, centralized management components, implementation services, training, and integration with the Corporation's networking, cybersecurity, monitoring, and application platforms.

Detailed technical requirements are provided in the Load Balancing Platform Compliance Matrix below.

Code	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
LB01	**Application Delivery Controllers (Quantity= 4)**		
General Requirements			
1.	The Solution shall adopt modern methods of service delivery allowing the Application Delivery Controllers to host multiple instances of the ADC service.		
2.	The OEM shall not be currently blacklisted by any Central/State Govt. dept. /Public Sector or any other regulatory bodies Unit.		
3.	The proposed appliance must be latest but stable solution and must not be END OF LIFE/END OF SUPPORT/END OF ENGINEERING SUPPORT (which includes all kind of support viz. Hardware, Software etc.)		
4.	The OEM shall provide 24x7x365 technical support, software updates, security patches and hardware replacement services for a minimum period of three (3) years.		
5.	The proposed solution shall be eligible for OEM hardware and software support extensions beyond the initial support term and shall not reach end-of-support within the next seven (7) years.		
6.	The proposed ADC platform shall support the enablement of the following capabilities without hardware replacement: a) Layer 4 and Layer 7 Load Balancing b) Global Server Load Balancing (GSLB) c) SSL/TLS Offloading d) High Availability and Clustering e) Application Health Monitoring f) DNS-based Traffic Management g) Content Caching and Compression h) Traffic Optimization and Acceleration i) Analytics and Reporting j) Centralized Management k) API-based Automation and Orchestration All capabilities shall be software-enabled and deployable without replacement of the proposed hardware appliances.		
7.	Vendor Training for personnel shall be provided, Certification Vouchers included		
8.	The tenderer shall design, implement, test and document a complete Disaster Recovery failover and failback procedure including witnessed DR testing and submission of test results.		
9.	Final acceptance shall be subject to successful completion of High Availability failover testing, Disaster Recovery failover testing, failback testing, GSLB functionality testing, performance validation and documentation sign-off.		
Technical Requirements			
10.	Hardware requirements for the ADC		

	L7 requests per second: 1.5M L4 connections per second: 1.1M L4 HTTP requests per second: 4M Minimum L4 concurrent connections: 4M Maximum L4 concurrent connections: 50M Throughput: 50 Gbps/50 Gbps L4/L7		
11.	Additional critical Specifications for the ADC: 7K TPS (2K SSL TPS) 5K TPS (ECDHE-ECDSA P-256 TPS) 5K TPS (ECDHE P-256-RSA-2k TPS) 8 Gbps bulk encryption		
12.	Proposed solution hardware specifications shall be vendor-defined, provided all performance, scalability, throughput, TPS, interface and high-availability requirements defined in this specification are met or exceeded. ADC Hardware Parts: 8-Core processor (4 CPUs available for Tenancy) 32 GB Random Access Memory, 480GB M.2 SSD 4 x 10G/1G RJ45 Ports, 4 x 25G/10G/1G SFP+/SFP28/SFP ports per device 1 x 250 W 100-240 VAC (+/- 10%) AUTO Switching Platinum, Dual PSU Management Ports: 1x 1000BASE-T, 1x USB 3.0, 1x serial console with auxilliary port		
13.	Proposed solution shall be able to support both Active/Active & Active/Standby deployment.		
14.	The proposed solution shall support deployment as two ADC appliances in the Primary Data Centre and two ADC appliances in the Disaster Recovery Data Centre, operating in High Availability mode within each site and Global Server Load Balancing mode between sites.		
15.	The Application Delivery Controller (ADC) shall support minimum ip-based persistency, session-based cookie persistency, headers inspection, URL redirection, and hash.		
16.	The solution shall continuously monitor application, server, network, DNS, WAN and site health and make traffic steering decisions based on configurable health monitoring policies.		
17.	The solution shall automatically redirect client traffic to the Disaster Recovery site in the event of application, server, network, or Primary site failure.		
18.	The solution shall support automatic and administrator-controlled failback of services to the Primary Data Centre upon restoration of normal operations.		
19.	The proposed solution shall include Global Server Load Balancing (GSLB) functionality capable of intelligent traffic distribution across the Primary Data Centre and Disaster Recovery Data Centre.		
20.	GSLB functionality and all licenses necessary for operation across the Primary and Disaster Recovery sites shall be included in the proposed bill of quantities.		

21.	The solution shall support authoritative DNS services and DNS response modification based on application health, geographic location, latency, persistence and site availability.		
22.	The solution shall support Kubernetes Ingress, Gateway API, OpenShift Routes, Helm Charts, ConfigMaps, Custom Resource Definitions (CRDs) and dynamic service discovery through a native container integration framework.		
23.	The solution shall support geographic load balancing, proximity-based routing, latency-based routing and site preference policies.		
24.	The Application Delivery Controller (ADC) must provide sophisticated monitors to check device, application, and content availability, including specialized monitors for many applications (including various application servers) as well as customized monitors to check content and simulate application calls.		
25.	The solution shall detect service failure and initiate failover within configurable intervals not exceeding 60 seconds.		
26.	The Application Delivery Controller (ADC) shall deliver sub-second system failover and comprehensive connection mirroring, resulting in a highly available solution regardless of system, server, or application failure. The system shall proactively inspect and respond to any server or application error.		
27.	The proposed ADC solution must perform Layer 4 through Layer 7 load balancing based on source/destination IP, application content, server weighting, TCP metrics, bandwidth utilization, response time and server health.		
28.	The ADC solution shall provide extensive connection management as well as TCP and content offloading capabilities that optimize server performance and dramatically speed page load times.		
29.	The ADC Solution shall provide intelligent caching functionality which helps to save tremendous cost by offloading repetitive traffic from web and application servers.		
30.	The proposed solution shall have feature of Caching with per service application, cache details and responses, dynamic content caching, push static content to local client machine and Customize Cache Timers option.		
31.	The Application Delivery Controller (ADC) must provide accelerated SSL encryption taking the burden of SSL off of the application servers. It also need to support SSL offloading.		
32.	The proposed solution shall support TLS 1.2 and TLS 1.3 and provide centralized certificate lifecycle management.		
33.	The solution shall support rate limiting connections for client to backend servers at the same time support TCP Surge protection, in an event of connection surge from end client the solution shall be able to queue the connection without dropping them.		
34.	The solution shall support gradual ramp up for new application servers allowing for easy onboarding of new application servers/instances		
35.	The proposed solution shall support multiple protocols like http, https, ftp, TCP, TCPS, SIP, Radius applications which can be configured with its own profile per service and be able to route the applications independently of server location or network schema, hence more applications will benefit from load balancer services		
36.	The solution shall support integration with enterprise identity providers including LDAP, Microsoft Active Directory, RADIUS,		

	TACACS+, SAML 2.0, OAuth 2.0, OpenID Connect (OIDC), ADFS and other industry-standard authentication mechanisms for administrator authentication, authorization and role-based access control.		
37.	The solution shall support HTTP and HTTPS connection pooling, multiplexing and reuse to optimize server resource utilization.		
38.	The proposed solution shall have the capability to configure multiple services on same Virtual IP with different ports and services options.		
39.	The proposed solution shall provide detailed charts and graphs to give more insight into the performance of web applications, with detailed views on HTTP and TCP stats, as well as system performance (CPU, memory, etc.)		
40.	The Application Delivery Controller (ADC) shall provide a highly targeted, centralized, and efficient means for reducing traffic volumes and minimizing the effect of latency and client connection bottlenecks on application performance. It shall support Application- centric configuration and analytics ensure optimized application performance.		
41.	Vendor must deliver successful installation, configuration, & integration for the proposed solutions in a datacenter environment, integrating with internal services that use digital signature.		
42.	Vendor shall atleast hold Authorised partnership or higher level of partnership with Manufacturer. Must present MAF for the product proposed.		
43.	The ADC Solution shall have the ability to condense HTTP traffic using industry-standard gzip and DEFLATE compression algorithms, or any other better algorithm to reduce bandwidth consumption and user download times over slower/low bandwidth connections. It should also provide a rich support for compressing a variety of file types, including HTTP, XML, JavaScript, J2EE applications, and many others.		
44.	The Application Delivery Controller (ADC) shall deliver the industry's most selective encryption to holistically, partially, or conditionally encrypt data, enabling secure and optimized communications with a variety of different constituencies.		
45.	The solution shall support integration with Health monitoring Tools based on SNMP v2 and above.		
46.	The solution shall support integration with Security Information and Event Management (SIEM) platforms		
47.	The solution shall provide templates that are used to define and tie all related application services and resources to the specific application being deployed. The application service object shall create a contextual view and advanced statistics of those services.		
48.	The solution shall provide analytics, shall capture application-specific statistics reported at different levels of the service, such as URL, throughput, and server latency, with views per virtual servers, pools, and nodes.		
49.	There shall be an option to set thresholds for some of the statistics, and an alert should be delivered via syslog, SNMP, or email when the threshold is exceeded. Analytics also should be configurable		

	through the templates, with the option to export the data off-box to a third-party remote logging/ reporting engine.		
50.	Device Service Clustering: There shall be an option for administrators to enable automatic syncing to keep applicable application and networking configuration information of all devices in a device group up to date.		
51.	The proposed system architecture shall provide the ability to scale up or scale out on demand, creating an elastic Application Delivery Controller (ADC) processing platform that can grow as the business needs change.		
52.	The proposed solution shall provide programmable traffic management capabilities through a policy engine, scripting framework, or equivalent mechanism, enabling Layer 4 through Layer 7 traffic inspection, content switching, header manipulation, URL-based routing, traffic steering and application delivery policy enforcement.		
53.	The proposed solution shall support Layer 4 through Layer 7 traffic inspection, content switching, payload transformation, header manipulation and policy-based traffic steering.		
54.	IPv6 Gateway (NAT64 support): The proposed solution should have a feature that provides complete IP transformation and load balancing capabilities between v4 and v6 networks. In addition to working with native IPv6 networks, it also should support the DNS64 and NAT64 standards for effective IPv4 to IPv6 translation.		
55.	High speed logging: The proposed solution shall have the ability to pass TCP or UDP log traffic at extremely high rates.		
56.	The proposed solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode		
57.	The proposed solution shall allow traffic management, load balancing, GSLB and application delivery services to be managed programmatically through declarative APIs.		
58.	The solution shall support API's and have an SDK that allows for automation and integration of custom applications into all aspects of the application delivery controller and any modules that run within the solution.		
59.	The solution shall provide secure REST-based APIs for all configuration, management, monitoring and reporting functions.		
60.	The solution shall support SDN services that natively support protocols such as VXLAN, NVGRE etc allowing for the bridging between traditional and virtual networks allowing for deployment of application delivery services across all types of environments.		
61.	The solution shall support advanced network routing capabilities such as BGP, RIP, OSPF, ISIS, and BFD for enhanced interoperability within the network, increasing the resilience and capacity of your network		
62.	The solution shall support integration with common automation tools such Chef, Puppet, Ansible and Terraform.		
63.	Centralized management platform shall provide configuration management, backup, compliance monitoring, software lifecycle management, analytics and role-based administration across all ADCs deployed in Primary and Disaster Recovery sites.		

64.	The solution shall provide automated configuration backup, version control and restore capabilities for all ADC and GSLB configurations.		
65.	The solution shall generate scheduled reports covering application availability, failover events, DNS steering events, capacity utilization and operational & system events.		
66.	The ADC shall provide TCP connection management and basic SYN protection mechanisms for service availability.		
67.	The solution shall support API load balancing and API traffic routing.		
68.	The solution shall support granular Role-Based Access Control (RBAC) integrated with LDAP, Active Directory, TACACS+ and RADIUS.		
69.	The solution shall maintain tamper-resistant audit logs for all administrative, configuration and policy changes.		
Licensing Requirements			
70.	Device shall come with perpetual licensing with a separate license subscription for support and software updates		
71.	Licensing shall permit centralized management and transfer of licenses between ADC instances without requiring hardware replacement.		
72.	The proposed solution shall include all software licenses, subscriptions, management components, clustering licenses, GSLB licenses, API access licenses and any other licenses required to meet all functional requirements listed in this TENDER.		

2.2.4.2.10.10 Enterprise Integration Platform Requirements

Code	Requirement Description	Bidder Response (Yes/No)	Comments
INTP01	**Core Integration & Orchestration**		
1	The platform shall support integration between enterprise applications, databases, data platforms, cloud services, OT systems, external systems, and third-party applications.		
2	The platform shall support synchronous, asynchronous, event-driven, streaming, micro-batch, and batch integration patterns.		
3	The platform shall provide API management, messaging, event streaming, workflow orchestration, and data integration capabilities within a unified platform.		
4	The platform shall provide workflow orchestration, process automation, dependency management, scheduling, exception handling, and automated recovery capabilities.		
INTP02	**API Management & Service Exposure**		
5	The platform shall support REST, SOAP, GraphQL, and other industry-standard API protocols with full lifecycle management capabilities.		
6	The platform shall provide API gateway capabilities including authentication, authorization, throttling, version management, policy enforcement, routing, and traffic management.		

7	The platform shall support OAuth2, OpenID Connect, JWT, API keys, certificates, and other industry-standard security mechanisms.		
8	The platform shall provide API monitoring, usage analytics, performance management, latency analysis, and reporting capabilities.		
9	The platform shall provide developer portals, API catalogues, documentation management, onboarding tools, and self-service integration capabilities.		
INTP03	**Messaging, Event Streaming & Data Transformation**		
10	The platform shall support enterprise messaging, message queues, event brokers, publish-subscribe architectures, guaranteed delivery, persistence, retries, and event replay capabilities.		
11	The platform shall support low-latency event streaming, real-time processing, back-pressure handling, and scalable event distribution.		
12	The platform shall provide data transformation, schema mapping, validation, enrichment, filtering, aggregation, routing, and mediation capabilities.		
13	The platform shall support Change Data Capture (CDC), log-based replication, real-time synchronization, and data movement capabilities.		
14	The platform shall provide visual design tools, low-code integration development capabilities, reusable templates, and reusable integration services.		
INTP04	**Connectivity, Security & Governance**		
15	The platform shall provide pre-built and custom connectors for ERP, CRM, databases, cloud platforms, file systems, collaboration platforms, and legacy systems.		
16	The platform shall support REST, SOAP, FTP/SFTP, JDBC/ODBC, OPC UA, OPC DA, Modbus, MQTT, and other industry-standard integration protocols.		
17	The platform shall support secure integration across on-premises, private cloud, public cloud, hybrid cloud, and external partner environments.		
18	The platform shall provide SDKs, development frameworks, and extensibility mechanisms for development of custom connectors and integrations.		
19	The platform shall support encryption in transit and at rest, role-based access controls, multi-tenancy, policy enforcement, data masking, audit logging, and compliance controls.		
INTP05	**Monitoring, Operations & Resilience**		
20	The platform shall provide centralized monitoring, observability, distributed tracing, log aggregation, request correlation, alerting, and operational analytics capabilities.		
21	The platform shall support integration with ITSM, incident management, monitoring, SIEM, and enterprise management platforms.		
22	The platform shall provide metrics and reporting capabilities for latency, throughput, utilization, error rates, service health, and integration performance.		

23	The platform shall support horizontal scalability, clustering, high availability, fault tolerance, workload balancing, and automatic failover capabilities.		
24	The platform shall support retry mechanisms, circuit breakers, fault isolation, resiliency patterns, and disaster recovery capabilities.		
25	The platform shall support DevOps and CI/CD practices including source control integration, automated testing, version management, deployment automation, and Infrastructure-as-Code (IaC) integration.		
26	The platform shall support deployment on shared enterprise infrastructure including physical, virtualized, containerized, cloud-native, and hybrid environments.		
INTP06	**Bidder Technical Proposal Requirements**		
27	The bidder shall provide the proposed Integration Platform architecture, including deployment across the Primary and Disaster Recovery Sites.		
28	The bidder shall provide the sizing methodology, assumptions, and calculations used to determine the proposed compute, storage, networking, messaging, API, and integration capacities.		
29	The bidder shall describe the proposed integration architecture, including API management, messaging, event streaming, workflow orchestration, data transformation, and connector strategy.		
30	The bidder shall describe the proposed scalability model, throughput characteristics, high availability architecture, disaster recovery approach, and performance optimisation strategy.		
31	The bidder shall describe the proposed security, governance, monitoring, observability, and operational management approach.		
32	The bidder shall describe the proposed integration approach with enterprise applications, databases, cloud services, OT systems, external partners, and third-party platforms.		
33	The bidder shall provide the proposed implementation methodology, migration approach, testing strategy, cutover plan, rollback procedures, knowledge transfer, and operational transition approach.		

2.2.4.2.10.11 Enterprise Monitoring and Response Platforms

The tenderer shall provide, install, configure, test, and commission an enterprise-grade Enterprise System Monitoring and Response Platform to provide centralized monitoring, observability, event management, performance monitoring, automation, and operational intelligence across the Corporation's Digital Transformation Platform.

The proposed solution shall provide a unified monitoring platform capable of monitoring enterprise infrastructure, applications, databases, networks, cloud services, containers, and operational technology (OT) environments. The platform shall deliver real-time visibility, proactive monitoring, automated response, operational analytics, and enterprise-wide observability to improve service availability, operational resilience, and business continuity.

The Enterprise System Monitoring and Response Platform shall:

ix. provide centralized monitoring, observability, and operational visibility across enterprise infrastructure, applications, databases, networks, cloud environments, and operational technology systems;
x. provide real-time monitoring of infrastructure health, application performance, user experience, service availability, and business-critical operations;
xi. support intelligent event correlation, anomaly detection, predictive analytics, automated incident response, and operational automation;
xii. provide centralized logging, metrics collection, distributed tracing, analytics, reporting, and compliance monitoring;
xiii. integrate seamlessly with enterprise cybersecurity, IT service management, DevOps, automation, and business continuity platforms;
xiv. support scalable, resilient, and highly available monitoring services capable of supporting future business growth;
xv. support automated asset discovery, dependency mapping, root cause analysis, SLA monitoring, and operational reporting; and
xvi. provide an OEM-supported Enterprise System Monitoring and Response Platform throughout the contract period.

The proposed solution shall include all software, licences, monitoring components, observability services, analytics capabilities, dashboards, automation services, implementation services, training, and supporting infrastructure required to deliver a fully integrated Enterprise System Monitoring and Response Platform.

Detailed technical requirements are provided in the Enterprise System Monitoring and Response Platform Compliance Matrix below.

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
1	Provide unified monitoring of infrastructure, applications, databases, containers, and cloud environments through a centralized management console		
2	Support real-time and near real-time metrics collection, event processing, and alerting with low-latency ingestion pipelines		
3	Support comprehensive observability including metrics, logs, and distributed tracing with end-to-end correlation capabilities		
4	Provide AI/ML-driven anomaly detection, predictive analytics, and trend analysis for proactive issue identification		
5	Support threshold-based, dynamic, and anomaly-based alerting with intelligent correlation and noise reduction mechanisms		
6	Integrate seamlessly with IT Service Management (ITSM) tools, ticketing systems, and workflow automation platforms		
7	Support event-driven automation, runbooks, and orchestration through integrations (e.g., Ansible, scripting frameworks)		
8	Provide automated dependency mapping, topology visualization, and root cause analysis capabilities		
9	Support application performance monitoring including instrumentation, transaction tracing, end-user monitoring, and synthetic testing		
10	Support both agent-based and agentless monitoring for operating systems, hypervisors, and hardware devices		

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
11	Provide native monitoring of containerized environments including clusters, nodes, pods, and services		
12	Support comprehensive network monitoring including devices, traffic flows, SNMP, NetFlow, sFlow, latency, and bandwidth utilization		
13	Provide centralized log management including collection, parsing, indexing, search, and integration with SIEM platforms		
14	Enforce security controls including role-based access control (RBAC), encryption (in transit and at rest), audit logging, and LDAP/Active Directory integration		
15	Provide customizable dashboards, KPI tracking, SLA monitoring, and report generation/export capabilities		
16	Support audit trails and compliance reporting aligned with applicable regulatory and industry standards		
17	Support logical data separation and fine-grained role-based access controls for multi-tenant or segregated environments		
18	Provide APIs and plugins for integration with CI/CD tools such as Jenkins, GitLab, and Terraform		
19	Support distributed architecture with clustering, horizontal scalability, and high availability		
20	Provide high-throughput ingestion pipelines capable of handling large-scale metrics, logs, and tracing data		
21	Support automated discovery of infrastructure, applications, services, and dependencies		
22	Provide AI-driven event correlation, deduplication, and alert suppression to improve signal-to-noise ratio		
23	Enable definition, monitoring, and reporting of SLAs/SLOs with alerts on threshold breaches		
24	Provide Real User Monitoring (RUM) and synthetic transaction monitoring capabilities		
25	Support extensibility through plugin frameworks, SDKs, and custom integrations		
26	Provide backup, replication, and failover mechanisms for the monitoring platform		
27	Support optimized compute utilization leveraging multi-core CPU architectures for analytics and ingestion workloads		
28	Support high memory utilization for in-memory processing, correlation, and indexing		
30	Ensure high availability through redundant components, clustering, and elimination of single points of failure		
31	Support monitoring of Operational Technology (OT) environments (e.g., SCADA, ICS) with secure integration and strict segregation between IT and OT domains		
32	Provide configurable incident response workflows, escalation matrices, and collaboration mechanisms for coordinated incident management		
33	Enable capacity planning, forecasting, and performance optimization using historical and predictive analytics		
34	Provide business service mapping and service-centric dashboards linking IT performance metrics to business KPIs and operational outcomes		

Item	Requirements Description	Tenderers Response (Yes/No)	Evidence Page
35	Support monitoring and reporting of disaster recovery posture, failover readiness, and RTO/RPO compliance		
36	Provide governance, risk, and compliance dashboards including policy monitoring, risk scoring, and regulatory reporting capabilities		
37	Provide unified security posture visibility through integration with SIEM, EDR/XDR, and vulnerability management systems		
38	Support monitoring of distributed, remote, and edge environments with capabilities for intermittent connectivity and centralized visibility		

2.2.4.2.10.12 Terminal Management System (TMS) Servers

Feature	KPC's Minimum Requirement	Tenderers Response (Yes/No)	Evidence Page
Server Architecture	x86 rack-mountable server from a well-known and recognized OEM brand.		
Processors	Two (2) Intel Xeon 6 Performance 6767P 2.4G, 64C/128T, 24GT/s, 336M Cache, Turbo, (350W) DDR5-6400		
Memory	Minimum 256 GB installed RAM using Registered DIMMs (RDIMMs). Must support at least 32 RDIMM slots. ECC memory protection required.		
Internal Storage	Support for at least 16 x Small Form Factor (SFF/2.5") drive bays.		
Installed Storage	Three (3) × 960 GB SSD SATA Mixed Use, 6 Gbps, 512e, 2.5", Hot-Plug, 3 DWPD.		
RAID Controller	Hardware RAID controller (Dell PERC 12 / PERC 13 series or equivalent). Must support RAID levels 0, 1, 5, 6, 10, 50, and 60. Controller card must include a minimum 8 GB battery-backed cache.		
Network and Fibre Interfaces	1. Two (2) × Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC. 2. Dedicated out-of-band management port (e.g. iDRAC / iLO) for remote access.		
PCIe Expansion	Minimum three (3) PCIe Gen expansion slots.		
Ports	1. **Front Ports: -** • 1 x USB 2.0 Type C port • 1 x USB 2.0 Type A port (optional) • 1 x Mini-DisplayPort (optional) • 1 x DB9 Serial (with front I/O configuration) • 1 x Dedicated ethernet port for iDRAC management 2. **Rear Ports: -** • 1 x Dedicated ethernet port for iDRAC management • 1 x VGA • 2 x USB 3.1 Type A ports Internal Ports: • 1 x USB 3.1 Type A port.		
Cooling	Minimum four (4) hot-plug fans.		
Power Supply	Dual hot-plug, fault-tolerant redundant (1+1) power supply units, minimum 700 W each.		
Hot-Swap Components	Drives, fans, and power supplies must all be hot-swappable.		

Operating Systems Supported	Must support: - VMware ESXi 7, 8, and 9. Ubuntu LTS; Citrix Hypervisor. Oracle Linux. Microsoft Windows Server LTSC with Hyper-V. Red Hat Enterprise Linux. SUSE Linux Enterprise Server.		
Security Features	Must include: - Cryptographically signed firmware. Data at Rest Encryption (SEDs with local or external key management). Secure Boot. Secure Erase. Secured Component Verification (hardware integrity check); Silicon Root of Trust; System Lockdown. TPM 2.0 (FIPS and CC-TCG certified).		
Warranty & Support	Three (3) years OEM hardware and software warranty. 24×7 remote support and 4-Hour Onsite Service		

2.2.4.2.11 Intrinsically Safe Tablets

Code	Feature	KPC's Minimum Requirement	Tenderers Response (Yes/No)	Evidence Page
TB 01	**Intrinsically Safe Tablets**			
1.	Hazardous Area & Environmental Certifications	**Explosion Proof Rating:** Device must be certified for Zone 1 and Zone 21 hazardous environments (ATEX / UKCA Ex certified: II 2G Ex db ia IIC T6 Gb IP64, II 2D Ex ia tb IIIC T80°C Db).		
		Ingress Protection: Minimum IP64 rating for dust and splash resistance.		
		Operating Temperature: Capability to operate within a temperature range of -20°C to +55°C.		
2.	Hardware & Processing	**Processor:** Octa-core 64-bit CPU (minimum 4 x 2.7 GHz)		
		System Memory: Minimum 4 GB RAM		
		Internal Storage: Minimum 64 GB internal storage with support for expandable Micro-SD storage up to 1 TB.		
		Display & Usability: High-brightness multi-touch screen operable while wearing industrial gloves, in wet conditions, and compatible with a passive/active stylus (S Pen).		
3.	Operating System & Software Support	**OS Version:** Android 12 or latest available version with Android Enterprise Recommended certification.		
		Enterprise Security: Built-in hardware/software security suite supporting biometrics (Facial Recognition).		
		Desktop Workstation Mode: Support for desktop-extension mode to allow external display docking for office/desktop workflows.		
4.	Connectivity & Communications	**Cellular Data:** 4G LTE-FDD / LTE-TDD, 3G UMTS, and 2G GSM support across major carrier networks.		
		Wireless Network: Wi-Fi 2.4 GHz + 5 GHz (IEEE 802.11 dual-band) with 2x2 MIMO, Wi-Fi Direct, and Hotspot capabilities.		
		Voice/Push-to-Talk: Integration support for Push-to-Talk over Cellular (PTToC) software and dedicated customizable active keys.		
5.	Imaging & Security Upgrades	**Primary Camera:** 13 MP auto-focus rear camera.		

Code	Feature	KPC's Minimum Requirement	Tenderers Response (Yes/No)	Evidence Page
		Front Camera 5 MP fixed-focus front camera.		

2.2.4.2.12 Ultra-Rugged Fixed RAIN RFID

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
ENV-01	RFID reader must feature industrial-grade dual IP65 and IP67 ratings for dust, spray, and water protection in extreme indoor and outdoor environments.		
ENV-02	Device must support an extended operating temperature range of -40°F to 149°F (-40°C to 65°C).		
ENV-03	Reader must meet MIL-STD-810 Method 514 (Procedure I) for vibration and MIL-STD-810H Method 509.7 for salt fog resistance.		
RF-01	High-sensitivity RF engine capable of long-range reads (minimum 12+ meters) with read speeds exceeding 1,000 tags per second.		
RF-02	Fixed reader must offer options with an integrated RFID antenna (7 dBi gain, 72° beamwidth) as well as 4-port and 8-port external RP-TNC configurations.		
RF-03	Integrated antenna models must achieve RFID read range of up to 100 ft (30.5 m) and a nominal read range of 55 ft (16.7 m).		
RF-04	Receiver sensitivity must reach a minimum of -92 dBm.		
WLAN-01	Integrated Wi-Fi radio must support IEEE 802.11ax/ac/a/b/g/n (Wi-Fi 6) 2x2 MU-MIMO with PHY data rates up to 1.2 Gbps on 5 GHz.		
WWAN-01	Device must support 5G/4G/3G cellular communications with dual SIM capability (1 Nano SIM and 1 eSIM). 4G/5G WWAN models are acceptable and CBRS support is not mandatory; readers shall operate in the approved unlicensed RFID band in Kenya, with SIM/eSIM from leading Kenyan operators where cellular connectivity is used.		
WPAN-01	Built-in Bluetooth must support Class 1, Bluetooth v5.3 with BLE, and Tap-to-Pair via NFC Tag.		
GPS-01	Reader must include integrated GNSS supporting GPS, GLONASS, BDS, Galileo, and QZSS.		
PWR-01	System must support versatile power options including PoE (802.3af), PoE+ (802.3at), direct 12–24 VDC flying leads, IP67 sealed AC/DC, IP67 sealed DC/DC, and standard indoor AC/DC.		
HW-01	Device hardware specs must include an NXP iMX8 Mini Quad Cortex-A53 CPU, 2 GB LPDDR4 RAM, 16 GB eMMC Flash, and Linux OS.		
SEC-01	System must support comprehensive security standards including Secure Boot, TLS 1.2/1.3, FIPS 140-2 cryptography, WPA3 Enterprise wireless security, SSH, and HTTPS administration interfaces.		
IO-01	Device must provide Gigabit Ethernet, 2 USB Host ports, 1 USB Client port, and 4 optically isolated General Purpose Inputs / 4 optically isolated General Purpose Outputs (GPIO).		

Code	Requirement Description	Tenderer Response (Yes/No)	Evidence Page
MNT-01	Reader must include standard flush mount and VESA mount options compatible with standard pole and hose clamp mountings.		

Quantity and placement: the BOM quantity of thirty (30) fixed RFID readers is a minimum. Tenderers shall distribute the readers based on their **site survey**; where the quantity is inadequate for the envisaged solution, the Tenderer shall add quantities to meet the requirements. All accessories required to make the solution functional – including but not limited to power and network cabling, masts complete with bases and civil works – shall be provided by the Tenderer. Additional site information shall be gathered during blueprinting.
Hazardous areas: all supplied equipment to be installed in Zone 2 (or more onerous) hazardous areas, as classified during the site visit, shall be ATEX/IECEx certified for that zone.

2.2.4.2.13 Industrial/Network Switches (5No)

Code	Feature	KPC Minimum Requirement specifications	Tenderers Response (Yes/No)	Evidence Page
NS01	**System Specifications**	Extreme 16801 or equivalent (5N0) At least 300 Gbps aggregate switch bandwidth/capacity At least 220 Mpps (Frame forwarding rate) Support at least 16000 MAC Address entries Support at least 8000 IP ARP entries Support at least 4000 IP Multicast entries Support at least 55000 IPv6 Route entries Support at least 11500 IPv4 Route entries Support 4000 VLAN's Support at least 248 routed interfaces *(Extreme 5420F model or equivalent)*		
NS02	**Port Configuration:**	At least 48 ports at 1 Gbps POE+, supporting high-density environments. MACsec capable ports Dedicated OOBM port at 1Gbs BASE-T Support Auto-sensing features for (AP, IP Phone, Camera, Printer, Data etc.) for dynamic port to VLAN assignments Support 8 QoS egress queues per port		
NS03	**Uplink Ports:**	4 x 10GbE SFP+ MACsec capable uplink ports for high-speed connectivity. The ports should be fully populated with 2*10GE SFP modules.		
NS04	**Power over Ethernet (PoE):**	Supports PoE+ with a power budget suitable for powering multiple devices such as IP cameras, phones, and access points.		

Code	Feature	KPC Minimum Requirement specifications	Tenderers Response (Yes/No)	Evidence Page
		Support a total POE budget of at least 1440W		
NS05	**Power Supply and Fans**	Support 1x internal fixed 860W PSU and 1x MUST have redundant hot-swappable PSU at 920W Internal fixed fan modules		
NS06	**Layer 3 Routing:**	Advanced Layer 3 routing capabilities include OSPF, BGP, and IS-IS. Support Static Routing		
NS07	**Security:**	Comprehensive security features including ACLs, 802.1X, and MAC security.		
NS08	**Management:**	Supports CLI, web-based, Central, SSH, RMON and Cloud management. Supports AI powered platform integration for quick MTTR (Mean-time-to-resolution), Insights, Configuration, Visualization, troubleshooting Support instant onboarding (ZTP)		
NS09	**Stacking:**	Support stacking up to 8 nodes for simplified management and increased scalability. Dedicated stacking ports At least 20Gb's stacking speed per port Supports channelization for non-used dedicated stacking ports		
NS10	**Automation:**	Includes support for automation, scripting and fabric technologies for streamlined network operations. Native fabric support without additional licensing.		
NS11	**Licensing and Support:**	Simplified and device agnostic Covered by limited lifetime warranty and include 3 years support Perpetual License		

2.2.4.2.13.1 Next-Generation Data Centre Firewalls (2 No.)

Model: Palo Alto PA-3440 or equivalent. The two firewalls shall be deployed as a high-availability pair at the primary data centre. No proof of concept is required for the firewalls.

Item	Minimum Requirement	Comply (Yes/No)	Bidder's Response
Make	Specify		
Model	Specify		
Operation	The NGFW platform must not experience performance degradation when all security features are turned on. The NGFW should be based on a single-pass parallel processing architecture for security processing. Decryption for TLS v1.3. Visibility into applications using non-standard ports. Must support App-ID, User-ID and Content-ID (or equivalent application, user and content identification).		
Performance and Interface Specifications	Threat prevention throughput of 20 Gbps (measured with application awareness, URL filtering, intrusion prevention, antivirus, sandboxing, file blocking and full logging enabled simultaneously). Firewall throughput 35 Gbps using both HTTP and AppMix. IPsec VPN throughput of 14.5 Gbps. Virtual systems (base/max) 1/11. 268,000 new sessions per second. 3 million maximum sessions. Interfaces: 12 x 10/100/1000 Mbps copper RJ45; 10 x 1/10G SFP/SFP+; 4 x 25G SFP28; 2 x 40/100G QSFP/QSFP28.		
Advanced URL Filtering	Block submission of corporate credentials to unknown or malicious sites. Enforce multi-factor authentication (MFA) and integrate with common MFA vendors to protect critical applications, including legacy applications containing sensitive data; MFA should not require a client on the client machine. Multi-category URL support; custom URL categories; real-time credential theft protection; phishing image detection; selective SSL decryption; search-engine cached results prevention; customisable end-user notifications; safe search enforcement; URL database. Protect against evasive techniques such as cloaking, fake CAPTCHAs and HTML character encoding. Cloud-based inline machine learning to analyse real web traffic and categorise and block malicious URLs in real time, with frequently retrained models protecting against new and never-before-seen threats (e.g. phishing, exploits, fraud, C2), and real-time protection from new malicious web pages.		
Machine-Learning-Powered Malware Prevention	Inline machine-learning-based malware and phishing prevention to stop most unknown attacks. Identify unknown malware and zero-day exploits using advanced static and dynamic analysis within the firewall without uploading samples to the cloud or a separate malware analysis platform. Zero-delay		

	(real-time) signature updates. The sandbox shall use machine learning, deep learning and YARA rules in static analysis; malware detonation, API hooking, behavioural analysis, recursive lookup and network IoC analysis in dynamic analysis; and dependency emulation, malware configuration extraction, intelligent runtime memory analysis and stealthy observation in advanced dynamic analysis.		
Next-Generation DNS Security	Machine-learning detection of domain generation algorithms (DGA), DNS tunnelling and command-and-control (C2), identifying threats hidden in DNS traffic; DGA analysis; real-time identification and blocking of previously unknown DGA-based threats; DNS sinkhole capability; DNS tunnel detection using machine learning on the behavioural qualities of DNS queries; detection and automatic blocking of C2 and data theft hidden in DNS tunnels; cloud-based DNS signatures and protection. Next-generation DNS security shall be in addition to the DNS filtering capabilities offered and licensed separately.		
Required Licences (3-year licence plan)	Advanced Threat Prevention; Advanced URL Filtering; Advanced DNS Security; Advanced WildFire (or equivalent sandboxing); Advanced SD-WAN; Device Security.		
Manufacturer Authorisation	Manufacturer's Authorisation Letter (as per the sample specified in the tender document).		
Supporting Documents	Technical literature/brochure supporting the supplied product.		
Deployment	Statement of Work (SoW) showing how the OEM will deploy the solution. The two firewalls shall be installed as a high-availability pair at the primary data centre. No firewalls are required at the terminal sites. IT/OT DMZ and OT firewalls are out of scope; the design shall integrate with the existing ones.		
Training (5 No.)	Certification training at a manufacturer-authorised training centre.		
Warranty	Three (3) years proactive and on-site warranty from the OEM, with Next Business Day (NBD) response.		

2.2.4.2.13.2 Reusable UHF RFID Tags

Parameter	KPC Minimum Technical Requirement	Comply (Yes/No)	Evidence Page
Type	Industrial-grade reusable passive UHF RFID tag for vehicle identification and tracking		
Quantity and use	150,000 tags, all for trucks (vehicle identification), complying with this specification		
Installation Surface	Must be suitable for installation directly on metallic surfaces		
Construction Material	Industrial-grade FR4 or better, resistant to normal outdoor and industrial operating conditions		
Tag Dimensions	Compact form factor inclusive of housing and protective casing		

Operating Frequency	UHF RFID operating within the unlicensed frequency band permitted for RFID operations in Kenya		
RFID Protocol / Standard	ISO/IEC 18000-63 and GS1 EPC Gen2 UHF RFID compliant		
Operation	Passive RFID, Read/Write		
Chip	RAIN RFID IC compliant with ISO/IEC 18000-63 and EPC Gen2v2, with minimum 128-bit EPC memory and read sensitivity of ≤ -23.5 dBm, or equivalent/better performance		
Memory	Minimum 128 bits		
Read/Write Range	Minimum 5–20 m when mounted on the intended surface, subject to reader, antenna and installation conditions		
Reader Compatibility	Compatible with both fixed and handheld UHF RFID readers		
Operating Temperature	-40°C to +100°C or better		
Storage Temperature	-40°C to +150°C or better		
Read/Write Endurance	Minimum 100,000 read/write cycles		
Service Life	Minimum 10 years under specified operating conditions		
Reusability	Tag shall be reusable and capable of being reassigned/reprogrammed as required		
Environmental Protection	Rugged construction suitable for outdoor and industrial oil logistics environments; minimum IP68 or better		
Mechanical Durability	Resistant to vibration, shock, impact and mechanical stresses associated with vehicle and logistics operations		
UV/Outdoor Resistance	Suitable for continuous outdoor exposure, including UV radiation, rain, dust and temperature variation		
Chemical Resistance	Tag housing shall be resistant to oils, fuels and commonly encountered industrial chemicals appropriate to the installation environment		
Identification	Each tag shall support a unique electronic identification number		
Printing / Marking	Blank, digital or permanently marked/printed identification as required		
Mounting	Suitable for secure mounting to metallic assets; mounting method appropriate for the asset and operating environment		
Data Retention	Minimum 10 years		
System Integration	RFID reader/middleware solution shall be capable of integration to the TMS through the specified integration interface/API		
Documentation	Manufacturer's technical datasheet shall be provided with the bid		
Manufacturer	Bidder shall state manufacturer, model and country of origin		

2.2.4.2.13.3 RFID Tag Printer / Encoder / Read-Writer

Parameter	KPC Minimum Technical Requirement	Comply (Yes/No)	Evidence Page

Type	Industrial/desktop UHF RFID reader-writer/encoder/printer suitable for programming reusable passive UHF RFID tags		
Primary Function	Shall read, write, encode, verify and reprogram compatible UHF RFID tags		
RFID Frequency	Must support the applicable locally configured unlicensed UHF RFID frequency band		
RFID Protocol / Standard	Shall support ISO/IEC 18000-63 (formerly ISO/IEC 18000-6C) and EPC Class 1 Gen 2 / Gen2v2, or later compatible standards		
Tag Compatibility	Must support the proposed M4QT or equivalent/better UHF RFID chip/tag		
Read/Write Capability	Read and write EPC, TID and User Memory where supported by the RFID tag		
Tag Reprogramming	Shall support repeated reassignment and reprogramming of reusable RFID tags		
Unique Identification	Shall read the tag's unique TID/electronic identification and associate it with the programmed EPC/vehicle record		
EPC Encoding	Shall support configurable EPC encoding appropriate for unique vehicle identification		
Memory Operations	Shall support reading, writing, locking and verification of supported tag memory banks		
Password Functions	Shall support Access and Kill password configuration where supported by the proposed RFID tag		
Encoding Verification	Shall automatically read back and verify programmed data to confirm successful encoding		
Anti-Collision	Shall support EPC Class 1 Gen 2 anti-collision functionality		
RF Power	Adjustable RF output power suitable for reliable encoding of individual tags without unintentionally programming adjacent tags		
Tag Isolation	Controlled/near-field encoding area or equivalent mechanism to ensure only the intended tag is programmed		
Metal-Mount Tag Support	Shall reliably read and program the proposed RFID tags, including tags designed for installation on metallic assets		
Interface	Minimum USB and Ethernet connectivity		
Host Compatibility	Compatible with current supported Microsoft Windows operating systems		
Software	Manufacturer's RFID configuration/encoding software shall be supplied		
SDK / API	SDK/API or documented integration interface shall be provided for integration with third-party applications		
TMS Integration	Encoded tag information shall be exchanged/integrated with the TMS; at minimum TID, EPC, vehicle identifier, commissioning status and date/time		
Duplicate Detection	Shall detect and prevent, or flag for user confirmation, duplicate EPC/TID assignments within the managed tag inventory		
Audit Trail	Auditable record of tag commissioning and reassignment, including TID, EPC, vehicle identifier, date/time, operator and programming/verification status		

Bulk Programming	Software should support sequential/batch tag commissioning and assignment where required		
Data Export	Export or exchange of programmed tag records in commonly used formats or through API/database integration		
Authentication / Access Control	Programming and tag-commissioning functions shall support controlled user access and authentication		
Power Supply	220–240 V AC, 50 Hz directly or through the manufacturer's supplied adapter, UK plug		
Accessories	All required cables, power adapters, antennas, mounting accessories and software/licences necessary for operation shall be supplied		
Documentation	Manufacturer's technical datasheet, user manual and SDK/API documentation shall be provided		
Manufacturer	Bidder shall state manufacturer, model and country of origin		
Warranty	Minimum three (3) years warranty, including on-site support		
Compatibility Requirement	Bidder shall demonstrate compatibility between the offered programmer/encoder and the proposed RFID tags		

2.2.4.2.13.4 75-Inch Outdoor Queue Display Screens

The thirty (30) outdoor queue display screens (TMS BOM item 2.1) shall meet the following minimum specification.

Parameter	Minimum Technical Requirement	Comply (Yes/No)	Evidence Page
Display Type	75-inch outdoor professional digital signage display		
Screen Size / Resolution	75-inch, 4K UHD, 3840 × 2160		
Display Technology	Direct LED, commercial-grade LCD		
Brightness	2,000 nits minimum		
Sunlight Suitability	Suitable for direct/full sunlight outdoor operation		
Environmental Protection	Minimum IP65. The displays are not required to be intrinsically safe (ATEX), but shall be installed outside classified hazardous zones		
Viewing Angle	178° horizontal / 178° vertical minimum		
Contrast Ratio	5,000:1 or better		
Panel Life	50,000 hours minimum		
Operating Temperature	-30°C to +40°C or wider		
Video Interface	HDMI 2.0 or better		
Network Interface	RJ45 Gigabit Ethernet		
Wireless Connectivity	Wi-Fi		
Audio	Integrated speakers		
Screen Protection	Anti-glare / outdoor protective glass		
Brightness Control	Automatic brightness control		
Thermal Management	Integrated outdoor thermal management system		
Operating Duty	Rated for 24/7 continuous commercial operation		
Integrated Computer	Integrated industrial PC or OPS PC		
Automatic Recovery	Automatic recovery/restart following power interruption or application failure		

Remote Management	PC shall support standard enterprise remote administration and software-management mechanisms		
Processor	Intel Core i5, 12th Generation or later, or equivalent/better		
Memory	16 GB RAM minimum		
Storage	512 GB NVMe SSD minimum		
Security	TPM 2.0 and Secure Boot		
PC Network Interface	Gigabit LAN		
PC Wireless Connectivity	Wi-Fi and Bluetooth		
Operating System	Genuine Microsoft Windows 11 Pro 64-bit, pre-installed and activated		
PC Display Capability	Capable of driving the display at 3840 × 2160 @ 60 Hz minimum		
PC Serviceability	PC accessible/serviceable without dismantling the complete display		
Mounting	Suitable for secure outdoor mounting using a manufacturer-approved mounting structure/bracket		
Accessories	All brackets, cabling, interfaces, power supplies and accessories required for a complete operational installation shall be included		
Civil and electrical works	The Tenderer shall provide display foundations, poles, shelters, civil works, electrical panels, surge/lightning protection and all other accessories necessary to make the solution operational		

2.2.4.3 *Common Enterprise Requirements*

The proposed Enterprise Digital Transformation Solution shall provide common capabilities and controls that apply across the enterprise applications, operational systems, shared services, data platforms, integration services and supporting infrastructure.

2.2.4.3.1 Workflow and Business Process Automation

The Solution shall provide configurable workflow and business process automation capabilities supporting the automation, routing, approval, escalation and monitoring of business processes.

Workflows shall support configurable business rules, approval hierarchies, segregation of duties, notifications, escalations, exception handling and audit trails without requiring extensive custom development.

2.2.4.3.2 User Access and Role Management

The Solution shall provide role-based access controls aligned with KPC's organisational structure, business functions and security policies.

Access shall be based on the principle of least privilege and shall support segregation of duties, role approval, role review, access revocation and periodic access certification.

The Solution shall support integration with KPC's Identity and Access Management environment.

2.2.4.3.3 Single Sign-On and Authentication

The Solution shall support integration with KPC's identity services and shall provide Single Sign-On (SSO) and Multi-Factor Authentication (MFA), where applicable.

The Solution shall support industry-standard identity and authentication protocols including SAML 2.0, OAuth 2.0, OpenID Connect, SCIM and LDAP, as applicable.

2.2.4.3.4 Audit Trails and Traceability

The Solution shall maintain comprehensive and tamper-resistant audit trails for significant user, system, configuration, workflow and transactional activities.

Audit information shall include, as applicable, user identification, date and time, transaction or activity performed, affected records, changes made and relevant system or process information.

Audit logs shall be available for authorised review and shall integrate with KPC's SIEM and security monitoring environment.

2.2.4.3.5 Segregation of Duties

The Solution shall support configurable Segregation of Duties (SoD) controls to prevent incompatible duties from being assigned to the same user or role.

The Solution shall provide capabilities for identifying, preventing, mitigating and reporting SoD conflicts in accordance with KPC's approved control framework.

2.2.4.3.6 Notifications and Alerts

The Solution shall provide configurable notifications and alerts for workflow activities, approvals, exceptions, system events, operational events, service conditions and other defined business or technical conditions.

Notifications shall support appropriate channels and shall be configurable according to user roles, business processes and event severity.

2.2.4.3.7 Enterprise Search

The Solution shall provide secure enterprise search and retrieval capabilities appropriate to each application and shared service.

Search functionality shall support relevant business records, documents, transactions and information while enforcing the access rights of the requesting user.

2.2.4.3.8 Reporting and Management Information

The Solution shall provide standard and configurable reporting capabilities across the enterprise.

Reports shall support operational, management and executive requirements and shall provide appropriate filtering, aggregation, drill-down, scheduling, export and dashboard capabilities.

Where information is sourced from multiple systems, reporting shall use approved enterprise data and integration services to ensure consistency and traceability.

2.2.4.3.9 Mobile and Self-Service Capabilities

Where applicable, the Solution shall provide secure mobile and self-service capabilities for employees, customers, suppliers and other authorised users.

Mobile and self-service functionality shall be integrated with the relevant enterprise processes and shall comply with KPC's security, access control and data protection requirements.

2.2.4.3.10 Master Data Management

The Solution shall provide capabilities for managing enterprise master data, including appropriate data ownership, stewardship, validation, approval, synchronisation and governance.

Master data shall be maintained consistently across integrated systems and shall support controlled creation, modification, approval and distribution.

2.2.4.3.11 Data Protection and Privacy

The Solution shall support the protection of personal, confidential, commercially sensitive and operationally critical information throughout its lifecycle.

The Contractor shall implement appropriate controls for data access, classification, retention, transmission, storage, processing and disposal in accordance with applicable KPC policies and the Kenya Data Protection Act, 2019.

2.2.4.3.12 Encryption and Cryptographic Security

The Solution shall protect data in transit and at rest using industry-recognised cryptographic standards.

Unless otherwise approved by KPC, data in transit shall be protected using TLS 1.2 or higher, while data at rest shall be protected using AES-256 or equivalent security controls.

2.2.4.3.13 Configuration and Change Management

The Solution shall provide controlled management of application, infrastructure, integration and security configurations.

All material changes shall be subject to KPC's approved change management processes and shall be appropriately tested, documented, authorised and traceable before deployment into production.

2.2.4.3.14 Performance and Scalability

The Solution shall provide adequate performance for KPC's current and projected user volumes, transaction volumes, data volumes and operational workloads.
The architecture shall support horizontal and/or vertical scalability, as appropriate, without requiring major redesign of the Solution.
The Contractor shall undertake performance and capacity testing before production deployment and shall provide sizing and capacity documentation.

2.2.4.3.15 Availability and Resilience

Critical components of the Solution shall be designed and implemented to minimise service disruption and single points of failure.
The Solution shall support appropriate high-availability, redundancy, failover, backup and recovery mechanisms in accordance with the approved architecture and business continuity requirements.

2.2.4.3.16 Monitoring and Observability

The Solution shall provide comprehensive monitoring and observability capabilities covering applications, infrastructure, databases, integrations, interfaces, services and relevant operational components.
Monitoring shall support performance monitoring, availability monitoring, capacity monitoring, event detection, alerting, logging and service health reporting.
Relevant monitoring information shall integrate with KPC's existing enterprise monitoring and security operations capabilities.

2.2.4.3.17 Interoperability and Open Standards

The Solution shall support standards-based interoperability and shall provide documented interfaces for integration with KPC's existing and future systems.
The Contractor shall provide complete and current API, interface, data exchange and integration documentation for all interfaces delivered under the Contract.

2.2.4.3.18 Configuration, Customisation and Extensions

The Contractor shall prioritise standard product functionality and configuration over custom development.
Any proposed customisation, extension or bespoke development shall be justified, documented, assessed for its impact on upgradeability and maintainability, and approved by KPC before implementation.

2.2.4.3.19 Documentation

The Contractor shall provide complete and current technical, functional, configuration, integration, security, operational and user documentation for all components delivered under Lot 2.
Documentation shall be updated throughout implementation and shall reflect the final production environment at handover.

2.2.4.3.20 Compliance with KPC Standards

All components of the Solution shall comply with KPC's applicable ICT, cybersecurity, architecture, data management, infrastructure, operational technology and service management standards and policies.
Where a proposed solution component cannot comply with an applicable KPC standard, the Contractor shall identify the deviation and obtain KPC's prior written approval before implementation.

2.2.5 Implementation Services

2.2.5.1 *Data Migration and Legacy System Transition*

The Contractor shall undertake the planning, preparation, execution, validation and completion of all data migration and legacy system transition activities required to implement the Enterprise Digital Transformation Solution.

The Contractor shall be responsible for ensuring that approved data is migrated accurately, securely, completely and in a manner that preserves data integrity, business continuity, historical information and required audit trails.

2.2.5.1.1 Migration Scope

The migration scope shall include, as applicable, data and relevant information from KPC's existing enterprise and operational systems, including the existing **SAP ECC6, SAP SRM and other identified legacy applications and platforms** within the approved project scope.

The Contractor shall assess and document the migration requirements for each source system, including the nature, volume, quality, structure, dependencies, retention requirements and business criticality of the data.

2.2.5.1.2 Data Migration Strategy

The Contractor shall develop a comprehensive Data Migration Strategy and Migration Plan covering:

a) source system assessment;
b) data inventory and profiling;
c) data ownership and stewardship;
d) data classification;
e) data quality assessment;
f) data cleansing;
g) data mapping;
h) data transformation;
i) data extraction;
j) data loading;
k) data validation and reconciliation;
l) migration testing;
m) cutover planning;
n) production migration;
o) post-migration validation;

The Migration Strategy shall be submitted to KPC for review and approval before production migration activities commence.

2.2.5.1.3 Data Profiling and Assessment

The Contractor shall undertake detailed profiling of data in the identified source systems to establish data completeness, accuracy, consistency, duplication, validity, structure and quality.

The Contractor shall identify data quality issues and agree with KPC on the appropriate cleansing, correction, transformation, archival or exclusion approach before migration.

2.2.5.1.4 Data Mapping and Transformation

The Contractor shall develop comprehensive source-to-target data mapping specifications for all migrated data.

The mapping shall identify the source data element, target data element, transformation rules, validation rules, data ownership and treatment of exceptions.

All transformation rules shall be documented and approved by KPC before execution of the production migration.

2.2.5.1.5 Master and Transactional Data

The migration shall cover approved master and transactional data required to support business continuity and the operation of the new Solution.

This may include, as applicable, customers, suppliers, materials, assets, employees, financial data, procurement data, contracts, projects, inventory, maintenance information, commercial data, operational information and other approved enterprise records.

The Contractor shall ensure consistency between migrated master data and related transactional data.

2.2.5.1.6 Historical and Archived Data

The Contractor shall identify historical data that must be migrated, retained, archived or made accessible following implementation of the new Solution.
Where historical information is not migrated into the transactional system, the Contractor shall provide an approved and secure mechanism for authorised users to access and retrieve such information for operational, audit, legal, regulatory and reporting purposes.

2.2.5.1.7 Data Cleansing

The Contractor shall perform data cleansing activities in accordance with approved KPC data quality rules and agreed business requirements.
Data cleansing shall address, as applicable, duplicate records, incomplete records, invalid values, inconsistent classifications, obsolete information, incorrect references and other identified data quality issues.
Material data cleansing decisions shall be agreed with the relevant KPC data owners before implementation.

2.2.5.1.8 Migration Cycles

The Contractor shall undertake multiple migration cycles before final production migration.
Migration cycles shall progressively validate data extraction, transformation, loading, reconciliation, system functionality and business acceptance.
The Contractor shall incorporate lessons and defects identified during each migration cycle into subsequent cycles.

2.2.5.1.9 Data Reconciliation and Validation

The Contractor shall provide comprehensive reconciliation between source and target systems.
Reconciliation shall include appropriate record counts, financial values, transaction balances, master data, control totals and other agreed validation measures.
Any discrepancies identified during reconciliation shall be investigated, resolved and documented before migration acceptance.

2.2.5.1.10 Transition of KPC Legacy Systems

The Contractor shall develop and execute a controlled transition approach for KPC's legacy systems within the approved scope.

The transition shall address relevant master data, transactional data, open transactions, historical information, interfaces, configurations, reports, and other dependencies required to ensure continuity of KPC's business processes.

The Contractor shall ensure that the transition is executed in a controlled manner without loss of required business information or material disruption to KPC operations.

2.2.5.1.11 Data Security

All data migration activities shall be conducted in accordance with KPC’s information security, access control and data protection requirements.
The Contractor shall ensure that migrated data is protected against unauthorised access, disclosure, alteration, loss or destruction during extraction, transfer, transformation, loading, testing and storage.
Temporary migration datasets shall be securely managed and securely disposed of when no longer required.

2.2.5.1.12 Migration Testing

The Contractor shall conduct migration testing using representative datasets before production migration.
Migration testing shall validate data completeness, accuracy, transformation rules, business process functionality, interfaces, reports, controls and reconciliation.
Migration defects shall be documented, prioritised, resolved and retested before approval of the corresponding migration cycle.

2.2.5.1.13 Cutover and Production Migration

The Contractor shall prepare a detailed cutover plan covering migration sequencing, system freeze periods, data extraction, transformation, loading, reconciliation, validation, business readiness, contingency arrangements and go-live activities.
The final production migration shall only commence following KPC approval of the cutover plan and confirmation of readiness.
The Contractor shall provide sufficient technical and functional resources during the cutover and post-migration validation period.

2.2.5.1.14 Migration Contingency and Rollback

The Contractor shall provide documented contingency and rollback procedures for production migration.
The procedures shall identify conditions requiring rollback, decision-making authority, recovery steps, data restoration procedures and responsibilities.
The Contractor shall demonstrate the feasibility of the rollback approach during migration rehearsals where required by KPC.

2.2.5.1.15 Migration Deliverables

The Contractor shall provide, at a minimum, the approved Data Migration Strategy, Data Migration Plan, data inventory, data quality assessment, source-to-target mapping specifications, transformation rules, migration scripts and tools, migration test results, reconciliation reports, cutover plan, rollback plan, production migration report and final migration acceptance documentation.
All migration documentation shall reflect the final production environment and shall be handed over to KPC as part of the project documentation and knowledge transfer.

2.2.5.2 *Implementation, Testing and Deployment*

The Contractor shall provide all services necessary to implement, integrate, test, commission and deploy the Enterprise Digital Transformation Solution into a fully operational production environment.
The implementation shall be undertaken in a controlled and phased manner, with appropriate governance, quality assurance, testing, business readiness and KPC approvals at each stage.

No implementation shall disrupt the current business setup at any stage other than the cut-over stage where the necessary change management procedures and approvals will have been made.

2.2.5.2.1 Mobilisation and Project Initiation

The Contractor shall mobilise the required project resources, establish the implementation team and initiate the project in accordance with the approved implementation plan.
The Contractor shall undertake project initiation activities including resource mobilisation, project governance, detailed planning, stakeholder engagement, implementation scheduling, dependency identification, risk management and establishment of project controls.

2.2.5.2.2 Requirements Validation

The Contractor shall validate the requirements provided by KPC against the proposed solution.
The requirements validation shall confirm functional requirements, technical requirements, integrations, data requirements, reporting requirements, security requirements, infrastructure requirements and other implementation dependencies.
Any identified gaps, assumptions or deviations shall be documented and submitted to KPC for approval.

2.2.5.2.3 Detailed Solution Design

The Contractor shall develop detailed functional and technical designs for the Solution.

The designs shall cover, as applicable, business processes, application configuration, workflows, reports, integrations, data structures, security controls, infrastructure, interfaces, user roles, system environments and operational procedures.
Detailed design shall be subject to KPC review and approval before configuration or development of the corresponding components.

2.2.5.2.4 Infrastructure Deployment

The Contractor shall supply, install, configure and commission all infrastructure required for the Solution in accordance with the approved infrastructure architecture.
This shall include, as applicable, compute, storage, virtualization, containerization, databases, operating systems, load balancing, monitoring, backup, disaster recovery and other supporting infrastructure.
The Contractor shall undertake infrastructure sizing, installation, configuration, performance validation and documentation.

2.2.5.2.5 Solution Configuration and Development

The Contractor shall configure the proposed applications and platforms in accordance with the approved To-Be processes and detailed solution designs.
Where approved custom development is required, the Contractor shall undertake the necessary software development, configuration, testing, documentation and deployment activities.
All custom developments shall comply with approved development standards and shall not compromise the upgradeability, security or maintainability of the Solution.

2.2.5.2.6 Integration Development and Testing

The Contractor shall develop, configure and test all interfaces required to integrate the Solution with KPC's existing and future systems.
Integration activities shall include interface design, development, configuration, data exchange, error handling, security controls, monitoring, logging and end-to-end testing.

System Integrate	Purpose	Vendor/Version	Datasets	Notes/Protocols
SCADA / Historian to MSOOS and TMS and Analytics Platform	1. Condition monitoring for equipment 2. Actualizing Pump over 3. Mainline Schedule. 4. Analytics and Reporting 5. Batch tracking	Aveva/Schneider Electric	Nominations, Metered Quantities, Equipment status (Maintenance) , SCADA Historian data	OPC DA for real-time data; ODBC/SQL for historian/database access.
Automatic Tank Gauging (ATG) to MSOOS	Inventory Management	Rosemount / Emerson	Tank Inventory Data	ODBC connection to SQL Database
TAS - FuelFACS/Honeywell to MSOOS and TMS	Order fulfilment	Guidant	Loading orders; master data; transaction status; density; loading results	ODBC/SQL, file interfaces including SFTP/Robocopy
GIS to ERP	Linear asset data capturing		Depot/station locations; tanks; pipelines; routes; infrastructure/assets; geospatial coordinates	REST/API, OGC services, database connection or file exchange

System Integrate	Purpose	Vendor/Version	Datasets	Notes/Protocols
Preset / Batch Loading Controller to TMS	Order to Cash Execution,	Smith Meter AccuLoad	Order data, metered quantities, density & temperature	SMIP / Smith Meter protocol and/or Modbus TCP
Automatic Number Plate Recognition (ANPR) to TMS	Order Fulfilment		Vehicle Number plates, Timestamps (entry&exit)	REST API
Biometric / Access Control System to ERP	Staff Identification		Staff identification; access events; clock-in/out; driver access events; authentication results	API / database / file interface
TeamMate+/ Arbutus to All Proposed Solutions	Enable Real time Auditing		Audit transactions; operational/financial data;	ODBC/database connections, adapters, scripts, file imports
KRA iCMS to MSOOS	1. Order Fulfilment 2. Gate passing 3. Duty confirmation		Loading booking data; loaded quantities; gate-pass information; customs/transaction information	SOAP/XML web service (iCMSService), with Action identifying the transaction and RequestMsg carrying the XML business payload in CDATA.
KRA eTIMS to MSOOS and ERP	ETR Invoicing		Invoice information; tax invoice data; fiscalization/transaction information	RESTful web service using HTTP POST, transmitting invoice data in JSON format.
KRA iTAX to ERP and e-Procurement	File Tax Return Supplier Registration Compliance		Withholding tax/VAT, Payment Registration Number	File download
Banks to ERP	1. Payment Execution 2. Auto reconciliation 3. Bank statement		Payment transactions; account statements; MT940/MT942; payment confirmations; reconciliation data	SFTP/file exchange, API, IDOC
Hydrant Management Systems to MSOOS	Order fulfilment		Hydrant loading orders; loading authorization; metered quantities; transaction status	ODBC/database

System Integrate	Purpose	Vendor/Version	Datasets	Notes/Protocols
Integration of Security Information and Event Management (SIEM) to all proposed solutions	1. Real time Security events Monitoring. 2. Correlations	Fortinet	Security events; authentication events; application logs; API logs; audit trails; network events; integration and middleware events; security alerts and incidents	Syslog; REST API; SIEM connectors; agent-based or agentless log forwarding; event streaming
Integration of Identity and Access Management (IAM) to all proposed solutions	1. Identity Management 2. Single Sign on (SSO) One Identity		User identities; employee accounts; roles; permissions; access rights; authentication events; provisioning and deprovisioning data	LDAP/Active Directory; SAML; OAuth 2.0; OpenID Connect; REST API; SCIM
EPRA to MSOOS	Order Fulfilment			API
OMCs Systems to MSOOS	Order Fulfilment			API
Ability to Extend to other third-party solutions				API

2.2.5.2.7 Testing Strategy

The Contractor shall develop and implement a comprehensive Testing Strategy and Test Plan covering all Solution components.

Testing shall be undertaken progressively and shall include, as applicable:

a) unit testing;
b) configuration and functional testing;
c) system testing;
d) system integration testing;
e) interface testing;
f) data migration testing;
g) performance and load testing;
h) security testing;
i) disaster recovery and business continuity testing;
j) regression testing;
k) User Acceptance Testing (UAT); and
l) end-to-end business process testing.

2.2.5.2.8 System Integration Testing

The Contractor shall conduct end-to-end System Integration Testing to demonstrate that the Solution components operate together as an integrated enterprise environment.

Testing shall cover business applications, MSOOS, TMS , data platforms, integration services, infrastructure, cybersecurity services and relevant OT and external system interfaces.
All identified defects shall be recorded, prioritised, resolved and retested before progression to the next implementation stage.

2.2.5.2.9 Performance and Capacity Testing

The Contractor shall undertake performance and capacity testing to demonstrate that the Solution can support the agreed user volumes, transaction volumes, data volumes, integrations and operational workloads.
The Contractor shall identify and resolve performance bottlenecks before production deployment.
The results of performance and capacity testing shall be documented and submitted to KPC for approval.

2.2.5.2.10 Security Testing

The Contractor shall undertake appropriate security testing of the Solution before production deployment.
Security testing shall include vulnerability assessment, application security testing, configuration assessment, access control validation, penetration testing where applicable and verification of security logging and monitoring.
All critical and high-risk vulnerabilities identified during testing shall be resolved or formally accepted by KPC before production deployment.

2.2.5.2.11 User Acceptance Testing

The Contractor shall support KPC in conducting User Acceptance Testing based on approved business scenarios and acceptance criteria.
The Contractor shall provide test environments, test data, test scripts, technical and functional support, defect management and resolution support.
UAT shall confirm that the Solution meets the approved business requirements and To-Be processes.
Production deployment shall not proceed until the applicable UAT requirements have been successfully completed and approved by KPC.

2.2.5.2.12 Defect Management

The Contractor shall maintain a centralised defect and issue management process throughout implementation and testing.
Defects shall be categorised according to severity and business impact and shall be tracked through resolution, retesting and closure.
No critical defect or unresolved issue that materially affects the operation, security, integrity or availability of the Solution shall remain open at production go-live unless expressly approved by KPC.

2.2.5.2.13 Go-Live Readiness

Before production deployment, the Contractor shall undertake a formal Go-Live Readiness Assessment covering:
a) completion of approved configuration and development;
b) completion of required testing;
c) resolution of critical defects;
d) completion of data migration readiness activities;
e) infrastructure readiness;
f) integration readiness;
g) cybersecurity readiness;
h) user and administrator training;
i) operational and support readiness;
j) availability of documentation;
k) disaster recovery readiness;
l) business readiness; and

m) cutover and rollback readiness.
The Contractor shall submit a Go-Live Readiness Report to KPC for approval.

2.2.5.2.14 Cutover and Go-Live

The Contractor shall execute the approved cutover plan and coordinate all technical and business activities required for production deployment.
The Contractor shall provide sufficient technical and functional resources throughout the cutover and go-live period.
The Contractor shall monitor the Solution continuously during the initial production period and promptly resolve any incidents or defects affecting business operations.

2.2.5.2.15 Hypercare and Stabilization

Following go-live, the Contractor shall provide dedicated hypercare and stabilisation services.
Hypercare shall include enhanced monitoring, incident resolution, defect correction, user support, performance optimisation, data validation, integration monitoring and operational support.
The Contractor shall progressively transition the Solution from hypercare to the agreed steady-state support arrangement following successful stabilisation.

2.2.5.2.16 Implementation Environments

The Contractor shall establish and maintain appropriate Development, Test, User Acceptance Testing and Production environments and, where required, Disaster Recovery environments.
The environments shall be appropriately segregated and secured, with controlled movement of configurations, code, interfaces and other deployable components between environments.

2.2.5.2.17 Implementation Documentation

The Contractor shall maintain complete implementation documentation throughout the project, including approved designs, configuration records, development documentation, test plans and results, defect registers, deployment records, migration records, operational procedures and final system documentation.
All documentation shall be updated to reflect the final production environment.

2.2.5.2.18 Implementation Acceptance

Each major implementation stage shall be subject to the applicable acceptance criteria defined in the Contract.
KPC shall have the right to review and verify the completeness, quality, functionality, performance, security and compliance of the deliverables before granting acceptance.
Completion of an implementation activity shall not constitute acceptance unless the applicable contractual acceptance requirements have been satisfied and formally approved by KPC.

2.2.5.3 *Training, Change Management and Knowledge Transfer*

The Contractor shall provide a comprehensive training, change management and knowledge transfer programme to ensure that KPC personnel are adequately prepared to adopt, operate, administer, support and sustain the Enterprise Digital Transformation Solution.

2.2.5.3.1 Training Strategy and Plan

The Contractor shall develop and submit a comprehensive Training and Knowledge Transfer Plan covering all Solution components and relevant categories of KPC users.
The plan shall identify training requirements, target user groups, training methods, training environments, training materials, training schedules, trainers, competency requirements and evaluation methods.
Training shall be aligned with the implementation sequence and shall be completed sufficiently in advance of the relevant system go-live.

2.2.5.3.2 End-User Training

The Contractor shall provide role-based training to KPC end users covering the business processes and functionality applicable to their respective roles.

Training shall include practical exercises using the configured Solution and representative business scenarios.
The Contractor shall provide sufficient training sessions to support effective user adoption across the relevant KPC locations and business functions.

2.2.5.3.3 Super User and Business Process Training

The Contractor shall establish and train designated KPC super users and business process champions.
Super users shall receive enhanced functional training enabling them to support business users, perform first-level troubleshooting, assist with process adoption and participate in continuous improvement activities.

2.2.5.3.4 Technical and System Administration Training

The Contractor shall provide detailed technical training for KPC ICT personnel responsible for administration, configuration, integration, infrastructure, security, databases, monitoring, backup, disaster recovery and support of the Solution.
Training shall enable KPC technical personnel to undertake routine administration, monitoring, troubleshooting, configuration and operational support activities.

2.2.5.3.5 Security and Access Management Training

The Contractor shall provide appropriate training to KPC personnel responsible for application security, user administration, identity management, privileged access, audit, security monitoring and other relevant cybersecurity functions.

2.2.5.3.6 Operational and OT Training

For MSOOS, TMS and other operational components, the Contractor shall provide role-based operational training for relevant KPC personnel responsible for pipeline, terminal, depot, truck loading and associated operational processes.
Where the Solution integrates with OT environments, appropriate training shall also be provided to personnel responsible for the relevant OT systems and interfaces.

2.2.5.3.7 Training Materials

The Contractor shall provide comprehensive training materials, including user manuals, process guides, quick reference guides, administrator manuals, technical manuals, training presentations, practical exercises and other relevant learning materials.
All training materials shall reflect the final configured Solution and KPC-approved business processes.

2.2.5.3.8 Change Management

The Contractor shall support KPC's organisational change management activities necessary to facilitate adoption of the new Solution.
The change management activities shall include stakeholder engagement, communication, business readiness, user awareness, adoption support, change impact assessment and management of identified adoption risks.
The Contractor shall coordinate change management activities with KPC's designated programme and change management structures.

2.2.5.3.9 Business Readiness

The Contractor shall support KPC in assessing business readiness before each applicable Go-Live.
Business readiness activities shall address user preparedness, process readiness, training completion, availability of business procedures, organisational readiness, support arrangements and other factors that may affect successful adoption.

2.2.5.3.10 Knowledge Transfer

The Contractor shall provide structured knowledge transfer to KPC personnel throughout the implementation rather than limiting knowledge transfer to the end of the project.
Knowledge transfer shall cover functional processes, application configuration, technical architecture, infrastructure, integrations, data, security, administration, monitoring, support, troubleshooting and operational procedures.

2.2.5.3.11 Mentoring and Practical Knowledge Transfer

The Contractor shall provide hands-on mentoring and practical knowledge transfer to designated KPC personnel through workshops, demonstrations, joint configuration, troubleshooting sessions, operational exercises and other appropriate methods.

KPC personnel shall be given reasonable opportunities to participate in relevant implementation and support activities to build internal capability.

2.2.5.3.12 Knowledge Transfer Documentation

The Contractor shall provide complete documentation necessary for KPC to independently operate and support the Solution.

The documentation shall include functional, technical, configuration, architecture, integration, security, operational, administration, backup, recovery and troubleshooting documentation.

2.2.5.3.13 Training Evaluation

The Contractor shall evaluate the effectiveness of training through appropriate assessments, practical exercises, user feedback and competency checks.

Where identified competencies are not achieved, the Contractor shall provide remedial training or additional support at no additional cost to KPC where the deficiency is attributable to the Contractor's training delivery.

2.2.5.3.14 Training Records and Completion

The Contractor shall maintain records of training delivered, participants, training dates, training materials, assessments and completion status.

Training completion shall form part of the applicable implementation and acceptance requirements.

2.2.5.3.15 Sustainability and Capability Transfer

The Contractor shall ensure that the training and knowledge transfer programme enables KPC to progressively reduce reliance on the Contractor for routine administration, operation and support of the Solution.

The Contractor shall provide a capability transfer plan identifying the skills and competencies to be transferred to KPC personnel and the activities required to achieve operational sustainability.

2.2.5.4 *Support, Maintenance and Warranty*

The Contractor shall provide comprehensive warranty, technical support, maintenance and operational assistance for the Enterprise Digital Transformation Solution following commissioning and throughout the applicable Contract and support period.

2.2.5.4.1 Warranty

The Contractor shall provide a comprehensive warranty covering all software, infrastructure, configurations, integrations, interfaces, custom developments and other components supplied and implemented under the Contract.

The warranty shall cover defects, errors, failures, configuration deficiencies, integration failures and other issues attributable to the Solution or the Contractor's implementation.

The Contractor shall correct defects identified during the warranty period at no additional cost to KPC.

2.2.5.4.2 Post-Implementation Support

The Contractor shall provide post-implementation support covering the enterprise applications, MSOOS, TMS, data and analytics platforms, integration services, infrastructure and other components delivered under Lot 2.

Support shall cover incident management, problem management, service requests, change requests, technical troubleshooting, performance management, application support, infrastructure support and integration support.

2.2.5.4.3 OEM Support

The Contractor shall maintain appropriate OEM support arrangements for all proposed software, infrastructure and technology components for the applicable support period.

OEM support shall include access to software updates, security patches, technical assistance, product support, defect resolution and other support services applicable to the proposed products.
The Contractor shall ensure that no unsupported or End-of-Life components are introduced into the production Solution.

2.2.5.4.4 Service Desk and Incident Management

The Contractor shall provide an appropriate service desk and incident management capability for the Solution.
The service management arrangement shall provide mechanisms for logging, categorising, prioritising, assigning, escalating, resolving and closing incidents and service requests.
KPC shall be provided with appropriate channels for submitting and tracking support requests.

2.2.5.4.5 Service Levels

The Contractor shall provide Service Level Agreements (SLAs) defining the applicable service availability, incident response times, resolution targets, escalation procedures, service reporting requirements and other service performance obligations.
The SLA shall distinguish between different incident priorities based on business impact and severity.
Critical incidents affecting critical business or operational services shall receive the highest level of priority and escalation.

2.2.5.4.6 Application Support

Application support shall cover functional and technical issues affecting the enterprise applications and operational systems.
The Contractor shall provide support for configuration issues, application errors, workflows, reports, interfaces, integrations, user access, performance issues and other application-related incidents.

2.2.5.4.7 Infrastructure Support

The Contractor shall provide support for the infrastructure components supplied under the Contract, including servers, storage, virtualization, databases, operating systems, container platforms, load balancing, backup, monitoring and other supporting infrastructure.
The Contractor shall coordinate with the relevant OEMs where escalation to OEM support is required.

2.2.5.4.8 Integration Support

The Contractor shall provide support for all integrations implemented under the Contract.
Integration support shall include monitoring of interfaces, investigation of failed transactions, message processing, data synchronisation, API availability, integration performance and resolution of integration-related incidents.

2.2.5.4.9 Security and Vulnerability Support

The Contractor shall provide ongoing support for security-related issues affecting the Solution.
The Contractor shall ensure timely application of approved security patches, vulnerability remediation, security updates and relevant OEM security fixes.
The Contractor shall cooperate with KPC's cybersecurity teams in investigating security events and addressing vulnerabilities affecting the Solution.

2.2.5.4.10 Preventive Maintenance

The Contractor shall undertake preventive maintenance activities necessary to maintain the availability, performance, security and reliability of the Solution.
Preventive maintenance shall include, as applicable, system health checks, capacity reviews, performance optimisation, software updates, security patching, database maintenance, infrastructure maintenance and review of system configurations.
Planned maintenance activities shall be coordinated with KPC and shall minimise disruption to business operations.

2.2.5.4.11 Corrective Maintenance

The Contractor shall correct defects, failures, errors and other deficiencies identified during the support period.
Corrective maintenance shall include investigation, root cause analysis, remediation, testing and controlled deployment of corrective changes.

2.2.5.4.12 Problem Management and Root Cause Analysis

For recurring or significant incidents, the Contractor shall undertake formal problem management and root cause analysis.
The Contractor shall identify the underlying cause, recommend corrective and preventive actions and implement approved measures to prevent recurrence.

2.2.5.4.13 Change and Release Management

All changes to the production Solution shall be managed through KPC's approved change and release management processes.
The Contractor shall ensure that changes are appropriately assessed, authorised, tested, documented and deployed.
Emergency changes shall be subject to appropriate emergency change procedures and subsequent documentation and review.

2.2.5.4.14 Performance and Capacity Management

The Contractor shall monitor Solution performance and capacity throughout the support period.
The Contractor shall identify emerging capacity constraints, performance degradation and other potential service risks and recommend appropriate corrective or preventive measures.

2.2.5.4.15 Backup and Recovery Support

The Contractor shall support the operation and maintenance of backup and recovery mechanisms implemented under the Contract.
The Contractor shall periodically validate backup integrity and support recovery testing in accordance with KPC's approved business continuity and disaster recovery arrangements.

2.2.5.4.16 Service Reporting

The Contractor shall provide periodic service reports covering, as applicable:

a) incidents and service requests;
b) response and resolution performance;
c) SLA compliance;
d) recurring incidents;
e) problem management;
f) system availability;
g) performance and capacity;
h) security vulnerabilities and patches;
i) preventive maintenance;
j) changes and releases;
k) outstanding issues; and
l) recommended improvement actions.

2.2.5.4.17 Knowledge Retention During Support

The Contractor shall maintain effective knowledge transfer throughout the support period and shall ensure that KPC personnel remain sufficiently informed of Solution configuration, changes, upgrades, known issues, troubleshooting procedures and operational practices.

2.2.5.4.18 Product Upgrades and Lifecycle Management

The Contractor shall advise KPC on relevant product releases, upgrades, patches and technology lifecycle changes affecting the Solution.
The Contractor shall support approved upgrades and ensure that such upgrades are appropriately assessed, tested and implemented without compromising existing functionality, integrations, security or data integrity.

2.2.5.4.19 Support Transition

At the conclusion of the applicable Contractor support period, the Contractor shall support an orderly transition of operational and support responsibilities to KPC or any successor service provider appointed by KPC.
The transition shall include transfer of relevant documentation, configuration information, support records, known issues, technical knowledge, licences, credentials where applicable, operational procedures and other information required for continuity of service.

2.2.5.5 *Deliverables and Acceptance*

The Contractor shall provide all deliverables necessary to demonstrate that the Enterprise Digital Transformation Solution has been fully designed, implemented, integrated, tested, commissioned, documented and accepted by KPC.

2.2.5.5.1 Deliverables

The Contractor shall provide, as applicable, the following deliverables:
a) Project mobilisation and implementation plans;
b) approved Solution Architecture and detailed technical designs;
c) approved functional designs and To-Be business process configurations;
d) configured enterprise applications and operational systems;
e) configured MSOOS and TMS solutions;
f) Integration to EDRMS and shared enterprise services;
g) Enterprise Data Platform, analytics, reporting and approved AI capabilities;
h) Enterprise Integration Platform and all approved interfaces;
i) cybersecurity and identity integration;
j) ICT infrastructure and associated configuration;
k) OT/IT integration components;
l) data migration strategy, mapping, migration tools, migration results and reconciliation reports;
m) testing strategy, test plans, test scripts and test results;
n) security, performance, disaster recovery and business continuity test results;
o) User Acceptance Testing results and sign-off documentation;
p) cutover and go-live plans;
q) production deployment and commissioning documentation;
r) training materials and training completion records;
s) knowledge transfer and capability development documentation;
t) system administration and operational manuals;
u) technical, functional and user documentation;
v) configuration and custom development documentation;
w) integration and API documentation;
x) backup, recovery and disaster recovery procedures;
y) warranty and support documentation;
z) as-built architecture and configuration documentation;
aa) final implementation and commissioning reports; and
ab) any other deliverables specified in the Contract, approved implementation plan or Bill of Materials.

2.2.5.5.2 Deliverable Review and Approval

All major deliverables shall be submitted to KPC for review and approval in accordance with the agreed implementation schedule.
KPC may review, comment on, reject or request amendment of any deliverable that does not meet the applicable requirements.
The Contractor shall incorporate KPC's comments and resubmit the deliverable within the agreed period.
Approval of a deliverable shall not relieve the Contractor of responsibility for compliance with the Contract or for correcting defects subsequently identified.

2.2.5.5.3 Functional Acceptance

Functional acceptance shall confirm that the implemented Solution performs the approved business processes and functional requirements in accordance with the approved To-Be processes and solution designs.
Functional acceptance shall be supported by successful completion of the applicable testing and User Acceptance Testing.

2.2.5.5.4 Technical Acceptance

Technical acceptance shall confirm that the Solution, infrastructure, integrations, security controls, databases, interfaces and other technical components have been implemented in accordance with the approved architecture, specifications and applicable technical standards.

2.2.5.5.5 Integration Acceptance

Integration acceptance shall confirm that all required interfaces operate correctly and securely and that data is exchanged accurately between the Solution, KPC systems, OT platforms and approved external systems.

2.2.5.5.6 Data Migration Acceptance

Data migration shall be accepted only after the Contractor has demonstrated that the approved data has been successfully migrated, validated and reconciled in accordance with the approved migration requirements.
Material discrepancies, data loss or unresolved data integrity issues shall prevent acceptance of the affected migration deliverable until satisfactorily resolved.

2.2.5.5.7 Infrastructure Acceptance

Infrastructure shall be accepted following successful installation, configuration, testing and commissioning and demonstration that the infrastructure meets the approved capacity, performance, availability, security, backup and disaster recovery requirements.

2.2.5.5.8 Go-Live Acceptance

Production go-live shall be subject to KPC approval following confirmation that the applicable functional, technical, integration, migration, security, infrastructure, training, documentation and business readiness requirements have been satisfied.

2.2.5.5.9 Final Acceptance

Final Acceptance shall be granted following successful completion of the implementation and stabilisation period and confirmation that:
a) all contracted Solution components have been implemented and commissioned;
b) all required integrations have been completed and tested;
c) approved data migration has been completed and reconciled;
d) required testing and UAT have been successfully completed;
e) critical and high-priority defects have been resolved or formally accepted by KPC;
f) required training and knowledge transfer have been completed;
g) all required documentation has been delivered and approved;
h) the Solution has achieved the agreed performance, availability and security requirements;
i) disaster recovery and business continuity requirements have been demonstrated;
j) operational and support arrangements are in place;
k) all agreed contractual deliverables have been completed; and
l) all other outstanding contractual obligations relating to implementation have been satisfactorily completed.
Final Acceptance shall not be deemed to have occurred solely by reason of the Solution being placed into production or being used by KPC.

2.2.5.5.10 Defects and Outstanding Items

Where defects, deficiencies or outstanding items are identified during acceptance, the Contractor shall correct or complete them within the period specified by KPC.
KPC may withhold acceptance of the affected deliverable or milestone until the identified defects or deficiencies have been satisfactorily resolved.

2.2.5.5.11 Acceptance Certificates

Acceptance of applicable deliverables and milestones shall be formally documented through acceptance certificates or other written confirmation issued in accordance with the Contract.
The Contractor shall not treat a deliverable or milestone as accepted unless the applicable acceptance has been formally confirmed by KPC.

2.2.5.6 *Implementation Milestones and Payment Schedule*

Payment shall be based on achievement, evidence and formal acceptance of measurable milestone outcomes and shall not be based solely on elapsed time, expenditure incurred, resource deployment, percentage of effort expended, delivery of equipment, submission of documents, or achievement of the planned milestone date.

Recommended Acceptance Gate Rules
1. No certificate = no milestone payment — A tenderer cannot claim a milestone solely because the scheduled date has been reached or the deliverables have been submitted.
2. All mandatory gate conditions must be satisfied — Where a milestone contains multiple mandatory acceptance conditions, all must be met.
3. Evidence must accompany the certificate — Milestone Completion Report; deliverable register; acceptance test results; defect register; Requirements Traceability Matrix where applicable; relevant test reports; updated project schedule; updated risk/issue register; evidence of KPC approvals; signed Milestone Acceptance Certificate; invoice.
Payment shall be based on achievement, evidence and formal acceptance of measurable milestone outcomes and shall not be based solely on elapsed time, expenditure incurred, resource deployment, percentage of effort expended, delivery of equipment, submission of documents, or achievement of the planned milestone date.
WBS → Deliverables → Acceptance Criteria → Acceptance Gate → Milestone → Evidence → Payment

2.2.5.6.1 Milestone Certification
KPC shall certify each milestone only after verification that the applicable deliverables and activities have been completed in accordance with the Contract.
Certification shall be based on objective evidence including approved deliverables, test results, completion reports, acceptance records and other documentation specified by KPC.

2.2.5.6.2 Payment Conditions
Payments shall be subject to:
a) achievement of the applicable milestone;
b) submission of the required milestone deliverables;
c) successful completion of the applicable testing and acceptance requirements;
d) formal certification by KPC;
e) submission of the required invoice and supporting documentation; and
f) compliance with all other contractual payment conditions.

2.2.5.6.3 Retention
KPC may retain **ten percent (10%) of each certified milestone payment** up to a maximum cumulative retention of **ten percent (10%) of the Contract Price**.
The retained amount shall be released upon:
a) Final Acceptance of the Services;
b) completion of all contractual obligations;
c) completion of knowledge transfer; and

d) resolution of all outstanding defects, deficiencies and other contractual obligations.
Where permitted under the Contract, KPC may accept an equivalent **Performance Security** in lieu of retention, subject to the terms and conditions stipulated in the Contract.

2.2.5.6.4 Relationship Between Milestones and Acceptance

Achievement of a technical or implementation milestone shall not constitute Final Acceptance of the Solution.
Each milestone shall be assessed against its specific deliverables and acceptance criteria, while Final Acceptance shall be subject to successful completion of the overall Solution, stabilisation period and all outstanding contractual obligations.

2.2.5.7 *Tenderer Response Requirements*

The Tenderer shall provide a clear and comprehensive response demonstrating how the proposed Enterprise Digital Transformation Solution meets the requirements of this Section.
The Tenderer shall respond to each applicable requirement and shall clearly distinguish between standard functionality, configuration, custom development, third-party products, OEM components and proposed professional services.

2.2.5.7.1 Solution Compliance

The Tenderer shall provide a completed compliance matrix identifying, for each requirement:
a) compliance status;
b) proposed solution component;
c) description of how the requirement will be met;
d) whether the capability is standard, configurable or requires custom development;
e) applicable assumptions and dependencies; and
f) reference to supporting technical documentation.
The Tenderer shall not respond with generic statements such as "complied", "available" or "supported" without providing sufficient information to demonstrate how the requirement will be satisfied.

2.2.5.7.2 Solution Architecture

The Tenderer shall provide a proposed high-level Solution Architecture showing the relationship between:

a) Enterprise Business Applications;
b) MSOOS;
c) TMS;
d) Enterprise Data Platform;
e) Enterprise Data Analytics and AI;
f) Enterprise Integration Platform;
g) Cybersecurity and Identity Services;
h) Infrastructure;
i) Disaster Recovery environment;
j) OT systems and interfaces; and
k) external systems and services.

2.2.5.7.3 Functional Solution

The Tenderer shall describe the proposed functional solution for each major solution component and identify the principal capabilities proposed to meet KPC's requirements.
The response shall identify any functional gaps, proposed workarounds, customisations or third-party components required to achieve compliance.

2.2.5.7.4 Integration Response

The Tenderer shall provide an overview of the proposed integration architecture and identify the major internal, external and OT integrations required.
The response shall identify the proposed integration technologies, protocols, interface types, security mechanisms, monitoring arrangements and responsibilities for each major integration.

2.2.5.7.5 Infrastructure Response

The Tenderer shall provide proposed infrastructure sizing and architecture covering the Primary Data Centre, Disaster Recovery environment and relevant non-production environments.

The response shall identify proposed compute, storage, virtualization, databases, operating systems, networking, load balancing, backup, monitoring, high availability and disaster recovery components.

2.2.5.7.6 Data Migration Response

The Tenderer shall provide its proposed data migration methodology covering source system assessment, data profiling, cleansing, mapping, transformation, migration, reconciliation, validation, testing, cutover and legacy system transition.

The response shall identify the proposed approach for migration from SAP ECC6, SAP SRM and other systems within the approved migration scope.

2.2.5.7.7 Implementation Methodology

The Tenderer shall provide a detailed implementation methodology covering mobilisation, requirements validation, solution design, infrastructure deployment, configuration, development, integration, data migration, testing, UAT, cutover, go-live, hypercare, stabilisation and transition to support.

The methodology shall identify key activities, dependencies, deliverables, quality controls, governance arrangements and proposed implementation resources.

2.2.5.7.8 Testing and Quality Assurance

The Tenderer shall provide a comprehensive testing approach covering functional, integration, performance, security, migration, disaster recovery and User Acceptance Testing.

The response shall describe the proposed defect management, test management, quality assurance and acceptance processes.

2.2.5.7.9 Training and Knowledge Transfer

The Tenderer shall provide a Training, Change Management and Knowledge Transfer Plan covering end users, super users, system administrators, technical teams, support teams and other relevant KPC personnel.

The response shall identify proposed training methods, training environments, materials, schedules, competency assessment and knowledge transfer arrangements.

2.2.5.7.10 Support and Maintenance

The Tenderer shall provide its proposed warranty, support and maintenance model, including:

a) service desk arrangements;
b) incident and problem management;
c) service levels;
d) escalation procedures;
e) OEM support arrangements;
f) preventive and corrective maintenance;
g) security patching;
h) product upgrades;
i) performance and capacity management; and
j) transition to steady-state support.

2.2.5.7.11 Deliverables

The Tenderer shall provide a proposed deliverables schedule identifying all major deliverables associated with design, implementation, migration, testing, deployment, training, documentation, commissioning, support and acceptance.

2.2.5.7.12 Assumptions and Dependencies

The Tenderer shall clearly identify all material assumptions, dependencies, prerequisites and exclusions affecting delivery of the Solution.

Any component, licence, infrastructure, integration, service or other requirement necessary for the complete operation of the proposed Solution shall be clearly identified and included in the relevant Bill of Materials.

2.2.5.7.13 OEM and Third-Party Components

The Tenderer shall identify all OEM products, third-party products, subcontracted services and other externally sourced components proposed as part of the Solution.

The Tenderer shall provide evidence of the required OEM authorisations, partnerships, certifications and support arrangements in accordance with the requirements of the TENDER.

2.2.5.7.14 Tenderer's Responsibility for Completeness

The Tenderer shall ensure that its proposal represents a complete and operational Solution.

Any omission, dependency or prerequisite necessary for the proper functioning, integration, security, performance or supportability of the proposed Solution shall be identified by the Tenderer and included in the appropriate BOM and pricing schedule.

2.2.5.8 *Solution Documentation*

The Contractor shall provide complete, accurate and up-to-date documentation for all components of the Enterprise Digital Transformation Solution.

The documentation shall be developed progressively throughout the implementation and shall reflect the final configured and operational Solution at the time of handover.

2.2.5.8.1 Solution Architecture Documentation

The Contractor shall provide complete architecture documentation covering, as applicable:

a) Enterprise Architecture;
b) Business Architecture;
c) Application Architecture;
d) Data Architecture;
e) Integration Architecture;
f) Technology and Infrastructure Architecture;
g) Security Architecture;
h) IT/OT Architecture;
i) Disaster Recovery Architecture; and
j) Deployment Architecture.

2.2.5.8.2 Functional Documentation

The Contractor shall provide functional documentation for all implemented business applications and operational systems.

The documentation shall include, as applicable:

a) configured business processes;
b) To-Be process flows;
c) workflows and approval processes;
d) business rules;
e) roles and responsibilities;
f) functional configurations;
g) reports and dashboards;
h) forms;
i) interfaces; and
j) other functional configurations relevant to the Solution.

2.2.5.8.3 Technical Documentation

The Contractor shall provide detailed technical documentation covering all software, infrastructure, databases, middleware, integration components, security components and other technology implemented under the Contract.

The documentation shall include configuration information, Technical Specifications/Terms of Reference, dependencies, interfaces, system parameters and other information required for administration and support.

2.2.5.8.4 Integration Documentation

The Contractor shall provide complete documentation for all integrations implemented under the Contract.

The documentation shall include interface specifications, API specifications, data mappings, message structures, protocols, authentication mechanisms, integration dependencies, error handling, monitoring and support procedures.

2.2.5.8.5 Data Migration Documentation

The Contractor shall provide complete documentation relating to data migration, including:

a) source system inventory;
b) data profiling results;
c) data quality assessment;
d) source-to-target mapping;
e) transformation rules;
f) migration procedures;
g) reconciliation procedures;
h) migration test results;
i) cutover procedures; and
j) final migration reports.

2.2.5.8.6 Infrastructure Documentation

The Contractor shall provide complete documentation for the infrastructure implemented under the Contract, including servers, storage, virtualization, containerization, databases, operating systems, networking, load balancing, backup, monitoring and disaster recovery.

The documentation shall include final configurations, equipment schedules, logical and physical diagrams, sizing information, dependencies and support arrangements.

2.2.5.8.7 Security Documentation

The Contractor shall provide documentation covering the security architecture and controls implemented for the Solution.

This shall include, as applicable, access control, roles and permissions, IAM integration, PAM integration, security configurations, encryption, audit logging, SIEM integration, vulnerability management and security monitoring.

2.2.5.8.8 Operational Documentation

The Contractor shall provide operational documentation required for the effective day-to-day operation of the Solution.

This shall include system administration procedures, monitoring procedures, backup and recovery procedures, incident handling, troubleshooting, maintenance procedures, escalation arrangements and operational checklists.

2.2.5.8.9 User Documentation

The Contractor shall provide appropriate user documentation for the implemented applications and operational systems, including user manuals, process guides, quick reference guides and other materials required for effective use of the Solution.

2.2.5.8.10 As-Built Documentation

At completion of implementation, the Contractor shall provide comprehensive **As-Built Documentation** reflecting the actual production environment.

The As-Built Documentation shall incorporate all approved changes made during implementation and shall supersede preliminary design documentation where applicable.

2.2.5.8.11 Documentation Standards

All documentation shall:

a) be provided in editable electronic format where applicable;

b) use clear and consistent terminology;
c) reflect the final implemented Solution;
d) identify relevant version and configuration information;
e) be maintained under appropriate document and version control; and
f) be updated to incorporate approved changes throughout the implementation.

2.2.5.8.12 Documentation Handover

Complete documentation shall form part of the Contractor's handover and acceptance obligations. KPC shall not be considered to have received a complete Solution until the required documentation has been delivered, reviewed and accepted in accordance with the Contract.

2.2.5.9 *Solution Licensing and Third-Party Dependencies*

The Contractor shall provide all software licences, subscriptions, platforms, middleware, databases, development tools, integration components, infrastructure software and other technology components required for the complete operation, support and maintenance of the Enterprise Digital Transformation Solution.

2.2.5.9.1 Licensing Requirements

The Contractor shall clearly identify the licensing model applicable to each proposed software product and technology component, including, as applicable:
a) Named User licensing;
b) Concurrent User licensing;
c) Enterprise licensing;
d) Subscription licensing;
e) Consumption-based licensing; and
f) any other applicable licensing model.

The Contractor shall clearly state the licence quantities, metrics, validity periods, renewal requirements and applicable restrictions for each proposed product.

2.2.5.9.2 Licence Completeness

The Contractor shall ensure that all licences and subscriptions required for the complete operation of the proposed Solution are included in the appropriate Bill of Materials.

The Contractor shall identify all dependencies between software products, platforms, databases, middleware, integration tools, infrastructure and other components.

No component necessary for the operation of the Solution shall be excluded on the basis that it is a prerequisite, supporting component or third-party dependency.

2.2.5.9.3 OEM Authorization

The Contractor shall provide evidence of valid OEM authorisation or partnership for the major software and technology products proposed under the Contract, where applicable.

The Contractor shall maintain the required OEM relationships throughout the applicable implementation, warranty and support periods.

2.2.5.9.4 Third-Party Products and Services

Where third-party products or services are proposed, the Contractor shall clearly identify:
a) the product or service;
b) the OEM or provider;
c) its purpose within the Solution;
d) licensing or subscription requirements;
e) support arrangements;
f) integration dependencies;
g) product lifecycle and support status; and
h) any associated renewal or recurring costs.

The Contractor shall remain responsible for the successful integration and operation of third-party components forming part of the proposed Solution.

2.2.5.9.5 Licence Management

The Contractor shall provide a complete licence register covering all software and technology products supplied under the Contract.
The licence register shall include licence type, quantity, entitlement, expiry or renewal date, support status, OEM and applicable restrictions.
The Contractor shall support KPC in maintaining accurate licence records throughout the Contract period.

2.2.5.9.6 Product Lifecycle

The Contractor shall provide information on the product lifecycle, OEM support roadmap, release strategy and upgrade policy for all major proposed products.
The Contractor shall ensure that the proposed products remain within supported OEM lifecycle throughout the applicable implementation and support period.

2.2.5.9.7 Licence Renewals

Where licences or subscriptions require periodic renewal, the Contractor shall clearly identify the renewal period, applicable renewal costs and conditions in the Commercial Schedule and Total Cost of Ownership.
The Contractor shall provide KPC with sufficient advance notice of all upcoming licence and subscription renewals.

2.2.5.9.8 Transfer and Continuity of Rights

The Contractor shall ensure that KPC receives all licence entitlements, subscriptions, certificates, keys, documentation and other rights necessary to lawfully operate the Solution for the contracted period.
Where licences are registered in the Contractor's or an implementation partner's name, the Contractor shall ensure that KPC retains uninterrupted operational rights for the Solution in accordance with the Contract.

2.2.5.9.9 Open and Proprietary Technologies

The Contractor shall clearly identify proprietary technologies, open-source components and other software dependencies incorporated into the Solution.
For open-source components, the Contractor shall identify applicable licences and ensure that their use does not impose obligations that conflict with KPC's ownership, security, confidentiality or operational requirements.

2.2.5.9.10 Licensing Documentation

The Contractor shall provide complete licensing documentation, including licence certificates, entitlement records, subscription details, OEM support agreements and applicable licence terms, as part of the Solution documentation and handover.

2.2.5.9.11 Licensing and Commercial Response

The Tenderer shall separately identify one-time and recurring licensing costs in the relevant Bill of Materials.
The Tenderer shall clearly distinguish between:
a) perpetual licences;
b) subscription licences;
c) annual maintenance and support;
d) cloud or consumption charges;
e) OEM support;
f) third-party licences; and
g) other recurring technology costs.
All licensing assumptions shall be clearly stated and shall form part of the Tenderer's Total Cost of Ownership.

2.2.5.10 *Enterprise Solution Security and Compliance*

The Contractor shall design, implement, configure and maintain the Enterprise Digital Transformation Solution in accordance with KPC's applicable information security, cybersecurity, data protection, regulatory and compliance requirements.

2.2.5.10.1 Information Security

The Solution shall incorporate security controls throughout the application, data, integration, infrastructure and Operational Technology environments.

The Contractor shall apply security-by-design principles throughout the Solution lifecycle and shall ensure that security requirements are addressed during design, development, configuration, testing, deployment and support.

2.2.5.10.2 Identity and Access Management

The Solution shall integrate with KPC's existing Identity and Access Management (IAM) platform and shall support centralised authentication and authorisation.

The Solution shall support role-based access control, least-privilege access, segregation of duties, user provisioning and de-provisioning, access review and appropriate authentication mechanisms.

2.2.5.10.3 Privileged Access Management

Administrative and privileged access to the Solution and supporting infrastructure shall integrate with KPC's Privileged Access Management (PAM) capabilities.

Privileged activities shall be appropriately controlled, monitored and auditable.

2.2.5.10.4 Security Monitoring and SIEM Integration

The Solution shall integrate with KPC's Security Information and Event Management (SIEM) platform.

Relevant application, infrastructure, database, integration, authentication, privileged access and security events shall be capable of being securely logged and forwarded to the SIEM for monitoring and analysis.

2.2.5.10.5 Security Logging and Audit

The Contractor shall configure comprehensive security and audit logging for the Solution.

Logs shall be appropriately protected against unauthorised modification or deletion and shall support investigation, compliance monitoring, incident response and audit activities.

The Contractor shall define appropriate log retention requirements in consultation with KPC.

2.2.5.10.6 Data Protection

The Contractor shall ensure that personal data and other protected information processed by the Solution are handled in accordance with the **Kenya Data Protection Act, 2019**, applicable regulations and KPC's information security and data protection requirements.

The Contractor shall implement appropriate controls for data collection, processing, storage, transmission, access, retention and secure disposal.

2.2.5.10.7 Data Sovereignty

Where the Solution or any component is hosted outside KPC-controlled infrastructure, the Contractor shall clearly identify the hosting location, service provider, data residency arrangements, processing locations and Disaster Recovery location.

The Contractor shall obtain KPC's approval for applicable hosting and data residency arrangements before deployment.

2.2.5.10.8 Encryption

The Contractor shall implement appropriate encryption for sensitive and confidential information. Data in transit shall use **TLS 1.2 or higher**, while data at rest shall use **AES-256 or equivalent** recognised cryptographic protection, where applicable.

Cryptographic keys shall be appropriately protected and managed.

2.2.5.10.9 Vulnerability Management

The Contractor shall establish and maintain vulnerability management processes covering all Solution components supplied or implemented under the Contract.

The Contractor shall undertake vulnerability assessments, security testing and remediation activities and shall promptly address identified critical and high-risk vulnerabilities.

2.2.5.10.10 Security Testing

The Contractor shall conduct appropriate security testing before production deployment and throughout the applicable support period.

Security testing shall include, as applicable, vulnerability assessments, penetration testing, application security testing, infrastructure security assessment, configuration reviews and validation of security controls.

The Contractor shall provide KPC with relevant security testing reports and remediation evidence.

2.2.5.10.11 Secure Software Development

All custom software, interfaces, integrations and developments undertaken under the Contract shall follow an appropriate **Secure Software Development Lifecycle (SSDLC)**.

The Contractor shall apply secure coding practices, source-code controls, vulnerability management, security testing and controlled release processes.

2.2.5.10.12 Cybersecurity Incident Management

The Contractor shall promptly support KPC in the identification, investigation, containment, remediation and recovery of cybersecurity incidents affecting the Solution.

The Contractor shall cooperate with KPC's cybersecurity and security operations teams and shall provide relevant technical information, logs, forensic evidence and remediation support where required.

2.2.5.10.13 IT/OT Security

The Contractor shall ensure that integrations between IT and OT environments are implemented using appropriate security controls and approved integration boundaries.

The Solution shall maintain appropriate segregation between enterprise IT and operational environments and shall prevent unauthorised access to critical OT systems.

2.2.5.10.14 Security Patch Management

The Contractor shall monitor relevant OEM security advisories and provide security patches and updates applicable to the Solution.

Security patches shall be assessed, tested and deployed through approved change management processes.

Critical security vulnerabilities requiring urgent remediation shall be escalated to KPC immediately.

2.2.5.10.15 Security Compliance Standards

The Solution shall support security controls aligned with **ISO/IEC 27001:2022** and, where applicable to OT environments, **IEC 62443**.

The Contractor shall provide evidence of compliance with applicable security standards, OEM certifications and security controls.

2.2.5.10.16 Compliance and Regulatory Requirements

The Contractor shall ensure that the Solution supports applicable Kenyan legal, regulatory and statutory requirements relevant to KPC's operations.

The Contractor shall identify material compliance requirements applicable to the proposed Solution and demonstrate how they are addressed through the proposed architecture, functionality, controls and implementation approach.

2.2.5.10.17 Security Documentation

The Contractor shall provide complete security documentation covering the implemented Solution, including security architecture, access controls, security configurations, integration with IAM, PAM and SIEM, encryption, logging, vulnerability management, security testing and incident response procedures.

2.2.5.10.18 Security Responsibilities

The Contractor shall clearly define the security responsibilities of KPC, the Contractor, OEMs, cloud providers and other third parties involved in delivering or supporting the Solution.

Where cloud or third-party services are proposed, the Contractor shall provide the applicable shared security responsibility model and identify the controls managed by each party.

2.2.5.11 *Operational Technology (OT) Integration*

The Contractor shall design, implement, configure, test and commission secure and reliable integration between the Enterprise Digital Transformation Solution and KPC's Operational Technology (OT) environment.

The OT integration shall support the exchange of approved operational data while maintaining the availability, integrity, confidentiality and security of KPC's operational systems.

2.2.5.11.1 OT Integration Scope

The scope shall include integration, as applicable, with KPC's existing and future OT platforms, including:

a) Supervisory Control and Data Acquisition (SCADA) systems;
b) Terminal Automation Systems;
c) Hydrant Management Systems;
d) OT/IT Firewalls;
e) OT Historians;
f) Operational Data Repositories;
g) Automatic Tank Gauging (ATG) systems;
h) Pipeline Integrity Management Systems (PIMS); and
i) other approved operational technology platforms.

2.2.5.11.2 OT/IT Integration Architecture

The Contractor shall develop a detailed OT/IT integration architecture defining the systems, interfaces, integration mechanisms, security boundaries, data flows and responsibilities for each integration.

The architecture shall maintain appropriate segregation between the enterprise IT environment and OT environment and shall not introduce unnecessary direct dependencies between critical OT systems and enterprise applications.

2.2.5.11.3 Secure Integration

All OT integrations shall be implemented using approved and appropriately secured integration mechanisms.

The Contractor shall implement appropriate authentication, authorisation, encryption, access control, monitoring, logging and network security controls for all OT interfaces.

2.2.5.11.4 Data Exchange

The Contractor shall identify and document the operational data required to be exchanged between OT systems and the Enterprise Digital Transformation Solution.

The data exchange shall be designed to maintain data accuracy, integrity, timeliness and traceability.

Where applicable, the Solution shall support near-real-time or real-time exchange of approved operational information without adversely affecting the performance or availability of the source OT systems.

2.2.5.11.5 Terminal and Loading Operations

The Contractor shall provide the required integration between the Terminal Management System and relevant operational systems supporting terminal and truck-loading activities.

The integration shall support, as applicable, loading orders, truck and driver information, loading bay allocation, loading status, operational transactions and other approved information required to support end-to-end terminal operations.

2.2.5.11.6 Pipeline Operations

The Contractor shall provide the required integration between the MSOOS and relevant pipeline operational systems.

The integration shall support approved operational information required for pipeline planning, scheduling, monitoring, hydrocarbon management, inventory management and other relevant midstream operations.

2.2.5.11.7 OT Data Historian and Operational Data

The Solution shall support controlled access to relevant historical and operational data required for enterprise reporting, analytics and decision support.

The Contractor shall ensure that extraction and use of OT data does not compromise the performance, availability or integrity of the source OT systems.

2.2.5.11.8 Integration Monitoring

All critical OT integrations shall be appropriately monitored.

Monitoring shall provide visibility of interface availability, transaction status, communication failures, data transmission errors and other conditions affecting the reliability of the integration.

Integration failures shall generate appropriate alerts and shall be capable of being investigated and resolved through defined support procedures.

2.2.5.11.9 OT Security and Access Control

Access to OT systems and OT data shall be strictly controlled based on authorised roles and approved business requirements.

The Contractor shall ensure that enterprise users and applications cannot obtain direct access to critical OT systems unless explicitly authorised and technically approved by KPC.

Privileged access to OT environments shall be controlled through KPC's applicable privileged access management and security controls.

2.2.5.11.10 OT Change Management

Changes affecting OT interfaces, integration components or OT-connected applications shall be subject to KPC's approved change management procedures.

The Contractor shall assess the potential operational and security impact of proposed changes before implementation.

Changes shall be tested in an appropriate non-production environment where technically feasible and shall be implemented during approved maintenance windows.

2.2.5.11.11 OT Availability and Resilience

The Contractor shall design OT integrations to minimise disruption to operational systems.

Failure of an enterprise application, integration component or external system shall not unnecessarily compromise the availability or safe operation of critical OT systems.

Where appropriate, the Contractor shall provide buffering, retry, queuing, failover and recovery mechanisms for critical integrations.

2.2.5.11.12 OT Integration Testing

The Contractor shall undertake comprehensive testing of all OT integrations before production deployment.

Testing shall include interface functionality, data accuracy, performance, security, failure handling, recovery, monitoring and end-to-end business process validation.

Testing shall be coordinated with the relevant KPC operational and technical teams.

2.2.5.11.13 OT Documentation

The Contractor shall provide complete documentation for all OT integrations, including architecture diagrams, interface specifications, data mappings, protocols, security controls, dependencies, configuration details, monitoring arrangements and operational procedures.

The documentation shall form part of the final As-Built Documentation.

2.2.5.11.14 OT Integration Governance

The Contractor shall comply with KPC's applicable OT governance, cybersecurity, safety, access control, change management and operational procedures.

No OT integration shall be implemented or materially changed without the required KPC review and approval.

2.2.5.12 *Solution Performance, Availability and Scalability*

The Contractor shall design, configure, implement and maintain the Enterprise Digital Transformation Solution to achieve the required levels of performance, availability, resilience and scalability throughout the Contract and applicable support period.

2.2.5.12.1 Performance Requirements

The Solution shall provide adequate performance for KPC's current and projected business, operational and transaction volumes.

The Contractor shall undertake appropriate sizing and capacity assessment based on user numbers, transaction volumes, data volumes, concurrent users, integration volumes, reporting requirements and expected future growth.

The Contractor shall identify all performance dependencies and shall ensure that no component of the Solution creates an avoidable performance bottleneck.

2.2.5.12.2 Response Time

The Solution shall provide acceptable response times for business transactions, user interfaces, workflows, reports, integrations and other system functions.

The Contractor shall propose measurable response-time targets for critical business processes and obtain KPC approval before implementation.

Performance targets shall be validated through appropriate performance and load testing before production deployment.

2.2.5.12.3 System Availability

Critical Solution components shall be designed to provide high availability and minimise unplanned service interruptions.

The Contractor shall identify availability targets for each major solution component and shall provide the necessary redundancy, clustering, failover and recovery mechanisms to achieve the approved availability requirements.

2.2.5.12.4 High Availability

Critical applications, databases, integration services and infrastructure components shall be configured with appropriate high-availability mechanisms.

The architecture shall minimise single points of failure and shall provide automatic or controlled failover where appropriate.

The Contractor shall test failover mechanisms before production deployment and periodically during the support period.

2.2.5.12.5 Scalability

The Solution shall be scalable to accommodate increases in:

a) users and concurrent users;
b) business transactions;
c) data volumes;
d) integration volumes;
e) reporting and analytics workloads;
f) operational workloads; and
g) additional business processes and solution components.

The Contractor shall clearly identify the scaling approach for each major component, including vertical and horizontal scaling where applicable.

2.2.5.12.6 Capacity Management

The Contractor shall establish capacity baselines and monitoring thresholds for the Solution.

Capacity management shall cover compute, memory, storage, databases, network resources, application workloads, integration services and other relevant components.

The Contractor shall periodically assess capacity utilisation and provide recommendations where additional capacity or optimisation is required.

2.2.5.12.7 Performance Monitoring

The Solution shall provide appropriate monitoring and performance management capabilities covering applications, infrastructure, databases, integrations and relevant operational components.

Performance monitoring shall support identification of bottlenecks, resource constraints, service degradation and emerging capacity issues.

2.2.5.12.8 Performance Testing

The Contractor shall conduct performance, load, stress and capacity testing appropriate to the Solution.

Testing shall demonstrate that the Solution can support the agreed user, transaction, integration and data volumes while maintaining the required performance and availability levels.

The Contractor shall submit performance test plans and results to KPC for review and approval.

2.2.5.12.9 Disaster Recovery Performance

The Disaster Recovery environment shall be appropriately sized to support the recovery of critical workloads within the approved recovery objectives.

The Solution shall support an **RPO of not more than thirty (30) minutes** and an **RTO of not more than two (2) hours** for critical workloads.

The Contractor shall demonstrate compliance through appropriate Disaster Recovery and failover testing.

2.2.5.12.10 Performance Optimisation

The Contractor shall investigate and resolve performance issues attributable to the Solution during implementation, warranty and support periods.

Where performance degradation is identified, the Contractor shall undertake root cause analysis and implement appropriate corrective or optimisation measures.

2.2.5.12.11 Availability Monitoring and Reporting

The Contractor shall provide periodic availability and performance reports covering the major Solution components.

Reports shall include, as applicable, system availability, outages, performance trends, capacity utilisation, significant incidents, recurring issues, service-level compliance and recommended corrective actions.

2.2.5.12.12 Scalability and Future Expansion

The Solution architecture shall support the addition of future users, business functions, depots, terminals, operational systems, integrations, data sources and digital services without requiring fundamental redesign of the overall architecture.

The Contractor shall identify the maximum supported capacity and recommended expansion thresholds for major Solution components and shall provide appropriate capacity planning information to KPC.

2.2.5.13 *Technical Performance Benchmarks*

The purpose of these Technical Performance Benchmarks is to establish the minimum performance, availability, scalability, security and resilience requirements that all proposed solutions must satisfy throughout implementation and operational use. These benchmarks provide objective performance standards against which the proposed solutions will be assessed to ensure they can reliably support business operations, integration requirements, operational growth, and future expansion.

The benchmarks are divided into two categories:

i. common technical requirements applicable to all systems, and
ii. specialized technical requirements specific to ERP, Midstream Oil Operations, E-Procurement, and Analytics & AI platforms.

Compliance with these benchmarks shall be validated through structured testing activities conducted prior to Go-Live.

2.2.5.13.1 Common Technical Requirements (Applicable to All Systems)

Availability and Reliability

Metric	Benchmark
System Availability	≥ 99.9%

Scheduled Maintenance Downtime	≤ 4 hours/month
Unplanned Downtime	≤ 45 minutes/month
Mean Time to Detect (MTTD)	≤ 15 minutes
Mean Time to Restore (MTTR)	≤ 4 hours

Response Time

Metric	Benchmark
User Login Time	≤ 5 seconds
Standard Screen Load Time	≤ 3 seconds
Dashboard Load Time	≤ 5 seconds
Search Query Response	≤ 3 seconds
Transaction Submission	≤ 5 seconds

Scalability

Metric	Benchmark
Concurrent Users	Support minimum 500-1,000 concurrent users
User Capacity Growth	Support 100% growth without redesign
Database Growth	Support 5-year projected data volume
Peak Load Performance	No degradation during peak transactions

Data Integrity

Metric	Benchmark
Transaction Success Rate	≥ 99.9%
Data Accuracy	≥ 99.9%
Record Processing Accuracy	≥ 99.9%
Duplicate Data Rate	≤ 0.1%

Security

Metric	Benchmark
Authentication Response	≤ 5 seconds
Vulnerability Severity (Critical)	Zero before Go-Live
Vulnerability Severity (High)	Zero unresolved
Audit Trail Capture	100%

Disaster Recovery

Metric	Benchmark
Recovery Time Objective (RTO)	≤ 2 hours
Recovery Point Objective (RPO)	≤ 30 minutes
Backup Success Rate	100%
DR Test Success	100%

2.2.5.13.2 ERP System Technical Benchmarks

Performance

Metric	Benchmark
Concurrent Users	1,000 users
Monthly Transaction Volume	≥ 1 million transactions
Purchase Order Processing	≤ 5 seconds
Invoice Processing	≤ 5 seconds
Financial Posting	≤ 3 seconds
Standard Report Generation	≤ 10 seconds

Complex Report Generation	≤ 60 seconds

Database Performance

Metric	Benchmark
Query Response	≤ 5 seconds
Batch Processing Jobs	≥ 95% completed within schedule
Period-End Processing	Complete within agreed business window

Integration Performance

Metric	Benchmark
API Response Time	≤ 2 seconds
ERP to External Systems Synchronization	≤ 5 minutes
Interface Success Rate	≥ 99.5%

2.2.5.13.3 Midstream Oil Operations System Technical Benchmarks

Real-Time Operations

Metric	Benchmark
SCADA/Field Data Capture Delay	≤ 30 seconds
Alarm Generation Time	≤ 60 seconds
Tank Inventory Update Time	≤ 1 minute
Pipeline Monitoring Refresh Rate	≤ 30 seconds
Operational Dashboard Refresh	≤ 1 minute

Large Volume Processing

Metric	Benchmark
Telemetry Processing Accuracy	≥ 99.9%
Throughput Calculations	≤ 1 minute
Daily Reconciliation Processing	≤ 15 minutes
Stock Reports Generation	≤ 5 minutes

Availability

Metric	Benchmark
Operational Monitoring Availability	≥ 99.95%
Critical Monitoring Module Availability	≥ 99.99%

2.2.5.13.4 E-Procurement System Technical Benchmarks

Transaction Performance

Metric	Benchmark
Supplier Registration Processing	≤ 10 seconds
Tender Publication	≤ 30 seconds
Tender Submission Upload	≤ 60 seconds
Bid Opening Process	≤ 2 minutes
Purchase Requisition Approval	≤ 5 seconds

Document Management

Metric	Benchmark
Document Upload (50MB)	≤ 30 seconds
Document Retrieval	≤ 5 seconds
Contract Search	≤ 5 seconds

Portal Performance

Metric	Benchmark
Concurrent Suppliers	≥ 5,000
Concurrent Internal Users	≥ 1,000
Portal Availability	≥ 99.9%

2.2.5.13.5 Analytics and AI Platform Technical Benchmarks

Analytics Performance

Metric	Benchmark
Dashboard Loading Time	≤ 5 seconds
Standard Report Execution	≤ 10 seconds
Complex Analytics Query	≤ 30 seconds
Ad-Hoc Query Response	≤ 15 seconds

Data Processing

Metric	Benchmark
ETL Success Rate	≥ 99.5%
Data Refresh Frequency	≤ 15 minutes
Data Warehouse Load Completion	Within scheduled window
API Data Ingestion Latency	≤ 5 minutes

AI Processing

Metric	Benchmark
Model Execution Time	≤ 10 seconds
Prediction Response Time	≤ 5 seconds
AI Service Availability	≥ 99.9%
Batch Model Processing	Complete within defined schedule

Benchmark Compliance Requirements

The proposed solution shall undergo Performance Testing, Load Testing, Stress Testing, Failover Testing, Backup and Recovery Testing, Disaster Recovery Testing, and User Acceptance Testing prior to Go-Live. The solution shall be considered compliant only upon demonstrating:

i. Compliance with not less than 95% of the specified performance benchmarks;
ii. 100% compliance with all security requirements;
iii. 100% compliance with all availability requirements;
iv. 100% compliance with all backup and recovery requirements; and
v. 100% compliance with all disaster recovery requirements.

All performance tests shall be executed using production-equivalent infrastructure, representative workloads, realistic transaction volumes, and integrated system interfaces.

2.2.5.13.6 Performance Testing and Acceptance Procedures

Objectives

The objectives of performance testing shall be to:

a) Verify that the solution meets the specified performance benchmarks.
b) Validate system stability under normal and peak workloads.
c) Confirm scalability to support future business growth.
d) Identify bottlenecks in infrastructure, applications, databases, and integrations.
e) Verify resilience and recovery capabilities.
f) Demonstrate readiness for production deployment.

Testing Environment Requirements

The Tenderer shall perform all tests using a production-equivalent environment.

Requirement	Minimum Requirement
Infrastructure	Production-equivalent sizing
Database	Same version as production
Network Configuration	Production equivalent
Security Controls	Production equivalent
Load Balancers	Production equivalent
Integrations	Connected to test interfaces or simulators
Test Data	Minimum three (3) years of representative business data

Integration Performance Testing

The Tenderer shall test all interfaces.

Test Scenarios

1. ERP - E-Procurement
2. ERP - Analytics Platform
3. ERP - Banking Platforms
4. ERP - HR Systems
5. Midstream Operations - ERP
6. Midstream Operations - SCADA/Telemetry Systems

Acceptance Criteria

Metric	Target
Successful Message Delivery	≥ 99.5%
API Response Time	≤ 2 seconds
Interface Failure Recovery	≤ 10 minutes
Data Synchronization Delay	≤ 5 minutes

Database Performance Testing

Validation Areas

- Query execution
- Bulk transaction processing
- Data archiving
- Index performance
- Reporting workloads

Acceptance Criteria

Metric	Target
Standard Query	≤ 5 seconds
Complex Query	≤ 30 seconds
Report Generation	≤ 60 seconds
Critical Deadlocks	Zero

Failover and High Availability Testing

The Tenderer shall demonstrate system resilience during component failures.

Scenario 1: Application Server Failure

Expected Result

a) Automatic failover;
b) No data loss.

Scenario 2: Database Node Failure

Expected Result

a) Automatic failover;
b) Continued operations.

Scenario 3: Network Link Failure
Expected Result

a) Automatic rerouting;
b) Service continuity.

Acceptance Criteria

Metric	Target
Failover Completion	≤ 5 minutes
User Service Impact	Minimal
Data Loss	Zero

Backup and Recovery Testing
The Tenderer shall successfully demonstrate the following recovery capabilities.
Test Scenarios

a) Full backup restoration
b) Incremental backup restoration
c) Database recovery
d) File recovery
e) Application recovery

Acceptance Criteria

Metric	Target
Backup Success Rate	100%
Recovery Time (RTO)	≤ 2 hours
Data Loss (RPO)	≤ 30 minutes
Recovery Validation	100% successful

Disaster Recovery Testing
The Tenderer shall conduct Disaster Recovery (DR) simulations and demonstrate recovery from the designated DR site.
Test Scenarios

a) Primary site outage
b) Database corruption
c) Infrastructure failure

Acceptance Criteria

Metric	Target
DR Activation Time	≤ 1 hour
Service Restoration	≤ 2 hours
Data Loss	≤ 30 minutes
Business Continuity	100% maintained

2.2.5.14 ***Business Continuity and Disaster Recovery***
The Contractor shall design, implement, configure, test and maintain comprehensive Business Continuity and Disaster Recovery capabilities for the Enterprise Digital Transformation Solution to ensure continuity and timely recovery of critical business and operational services following system failure, infrastructure failure, cybersecurity incidents, disasters or other disruptive events.

2.2.5.14.1 Disaster Recovery Architecture
The Contractor shall provide a Disaster Recovery environment capable of supporting the recovery of critical Solution components and services in accordance with the approved Solution Architecture and KPC's business continuity requirements.

The Disaster Recovery architecture shall provide appropriate replication, backup, recovery, failover, monitoring and restoration capabilities for critical applications, databases, integration services, data platforms and infrastructure.

2.2.5.14.2 Recovery Objectives

The Solution shall support a **Recovery Point Objective (RPO) of not more than thirty (30) minutes** and a **Recovery Time Objective (RTO) of not more than two (2) hours** for critical workloads.

The Contractor shall identify the applicable RPO and RTO for each major Solution component and shall demonstrate that the proposed architecture and technology can achieve the approved recovery objectives.

2.2.5.14.3 Business Continuity

The Contractor shall identify critical business processes and system dependencies and shall ensure that the Solution supports continuity of essential KPC operations during disruptive events.

Business continuity arrangements shall consider enterprise applications, MSOOS, TMS, data platforms, integration services, infrastructure, cybersecurity services and relevant OT interfaces.

2.2.5.14.4 Backup and Recovery

The Contractor shall implement appropriate backup and recovery capabilities covering application data, databases, configurations, system configurations, integration components and other critical information.

Backup arrangements shall provide appropriate backup frequency, retention, integrity protection, monitoring and secure storage.

The Contractor shall periodically verify the integrity and recoverability of backups.

2.2.5.14.5 Replication

Critical data and systems shall be replicated to the approved Disaster Recovery environment using appropriate technologies and mechanisms.

The replication solution shall support the approved recovery objectives and shall provide monitoring and alerting for replication failures, delays or inconsistencies.

2.2.5.14.6 Failover and Recovery

The Contractor shall provide documented and tested procedures for failover from the Primary Data Centre to the Disaster Recovery environment.

Recovery procedures shall cover infrastructure, databases, applications, integrations, data services, security services and other dependencies required to restore critical business services.

2.2.5.14.7 Disaster Recovery Testing

The Contractor shall conduct Disaster Recovery tests before production acceptance and periodically during the support period as agreed with KPC.

Testing shall demonstrate:

a) successful recovery of critical systems;
b) achievement of approved RPO and RTO;
c) integrity and availability of recovered data;
d) functionality of recovered applications;
e) availability of critical integrations;
f) effectiveness of failover and restoration procedures; and
g) readiness of KPC and Contractor support teams.

All test results, identified deficiencies and corrective actions shall be documented and submitted to KPC.

2.2.5.14.8 Recovery Procedures

The Contractor shall develop detailed recovery procedures covering the sequence and dependencies for restoring the Solution.

The procedures shall identify responsibilities, escalation mechanisms, technical recovery steps, validation activities and conditions for return to normal operations.

2.2.5.14.9 Return to Primary Environment

The Contractor shall provide documented procedures for controlled restoration of services from the Disaster Recovery environment to the Primary Data Centre following resolution of the disruptive event.
The return process shall include data synchronisation, validation, application recovery, interface verification and confirmation of business readiness.

2.2.5.14.10 Disaster *Recovery Documentation*

The Contractor shall provide and maintain a comprehensive Disaster Recovery Plan covering all critical Solution components.
The plan shall include architecture, system dependencies, recovery priorities, RPO and RTO requirements, backup arrangements, replication, failover procedures, recovery procedures, responsibilities, contact and escalation arrangements and testing requirements.

2.2.5.14.11 Cybersecurity and Disaster Recovery

The Disaster Recovery environment shall be subject to the same applicable security, access control, monitoring, logging and data protection requirements as the Primary Data Centre.
The Contractor shall ensure that Disaster Recovery mechanisms do not introduce unauthorised access or compromise the security of KPC data and systems.

2.2.5.14.12 OT Continuity

Where the Solution interfaces with OT systems, the Contractor shall ensure that Business Continuity and Disaster Recovery arrangements do not adversely affect the safe and reliable operation of critical OT systems.
The Contractor shall identify the recovery dependencies between enterprise systems and OT systems and shall provide appropriate recovery procedures for approved OT integrations.

2.2.5.14.13 Recovery Documentation and Knowledge Transfer

The Contractor shall provide practical training and knowledge transfer to designated KPC personnel on backup, recovery, failover, Disaster Recovery operations and business continuity procedures.
KPC personnel shall be provided with sufficient documentation and practical experience to participate effectively in recovery activities.

2.2.5.15 *Solution Governance and Change Control*

The Contractor shall establish and maintain appropriate governance and change control arrangements throughout the implementation, commissioning, warranty and support of the Enterprise Digital Transformation Solution.

2.2.5.15.1 Solution Governance

The Contractor shall participate in KPC's established project and technology governance structures and shall provide appropriate technical, functional and management representation throughout the Contract.
The Contractor shall ensure that all material decisions relating to architecture, configuration, integration, security, data, infrastructure, scope and technology are properly documented and subject to the applicable KPC approval processes.

2.2.5.15.2 Solution Governance Framework

The Contractor shall establish a governance framework covering:
a) solution architecture;
b) business process design;
c) application configuration;
d) integration;
e) data management;
f) infrastructure;
g) cybersecurity;
h) OT/IT integration;
i) testing and quality assurance;

j) change management;
k) release management;
l) risk and issue management; and
m) technical and operational support.

2.2.5.15.3 Design Authority

The Contractor shall establish appropriate design authority arrangements to ensure consistency and integrity of the overall Solution Architecture.
Material architectural decisions, deviations from approved designs and proposed technologies shall be documented and submitted to KPC for review and approval.
No material change to the approved architecture shall be implemented without the required KPC approval.

2.2.5.15.4 Change Control

All changes affecting the scope, functionality, architecture, configuration, interfaces, infrastructure, data, security or performance of the Solution shall be managed through an approved change control process.
Change requests shall clearly identify:
a) the proposed change;
b) reason and business justification;
c) affected systems and processes;
d) technical impact;
e) security impact;
f) data impact;
g) integration impact;
h) cost implications;
i) schedule implications;
j) risks and dependencies; and
k) testing and implementation requirements.

2.2.5.15.5 Change Approval

No material change shall be implemented without the appropriate approval in accordance with KPC's governance and delegated authority arrangements.
Approved changes shall be incorporated into the relevant project plans, configuration records, documentation and Bill of Materials where applicable.

2.2.5.15.6 Configuration Management

The Contractor shall maintain accurate configuration records for all Solution components.
Configuration management shall cover applications, infrastructure, databases, interfaces, integrations, security controls, system parameters and other components that may affect the operation of the Solution.
The Contractor shall maintain a controlled Configuration Management Database (CMDB) or equivalent configuration repository where required by KPC.

2.2.5.15.7 Release Management

The Contractor shall establish controlled release management procedures for application releases, patches, upgrades, configuration changes, integrations and other production changes.
Each release shall be appropriately assessed, tested, documented and approved before deployment.

2.2.5.15.8 Version Control

All applicable application code, configuration items, interfaces, technical documentation and other controlled artefacts shall be subject to appropriate version control.
The Contractor shall maintain records of approved versions and changes throughout implementation and support.

2.2.5.15.9 Risk and Issue Management

The Contractor shall maintain comprehensive registers for project risks, technical risks, issues, dependencies, assumptions and decisions.

Material risks and issues affecting scope, cost, schedule, security, performance, quality or operational continuity shall be escalated to KPC promptly.
The Contractor shall provide mitigation and corrective action plans for identified risks and issues.

2.2.5.15.10 Decision and Approval Records

The Contractor shall maintain appropriate records of material technical and implementation decisions, including the rationale, impact, approvals and resulting actions.
Such records shall form part of the project documentation and shall be handed over to KPC at completion.

2.2.5.15.11 Governance Reporting

The Contractor shall provide periodic governance reports covering, as applicable:
a) implementation progress;
b) milestone status;
c) risks and issues;
d) change requests;
e) defects;
f) testing status;
g) data migration status;
h) security matters;
i) integration status;
j) infrastructure readiness;
k) training and knowledge transfer;
l) outstanding decisions; and
m) matters requiring KPC action or approval.

2.2.5.15.12 Governance Compliance

The Contractor shall comply with KPC's approved governance, project management, architecture, security, change management, service management and operational procedures applicable to the Solution.
Where the Contractor proposes an alternative governance or control mechanism, it shall be subject to KPC's prior review and approval.

2.2.5.16 *Transition to Business-as-Usual Operations*

The Contractor shall provide a structured transition from implementation and stabilisation to business-as-usual operations to ensure that KPC can effectively operate, administer, support and maintain the Enterprise Digital Transformation Solution.

2.2.5.16.1 Transition Planning

The Contractor shall develop and submit a Transition to Business-as-Usual Plan covering the transition from implementation and hypercare to steady-state operations.
The plan shall define the activities, responsibilities, resources, timelines, dependencies, knowledge transfer requirements, support arrangements and acceptance criteria for the transition.

2.2.5.16.2 Operational Readiness

Before completion of the transition, the Contractor shall demonstrate that the Solution is operationally ready and that the required KPC teams, processes, documentation, tools and support arrangements are in place.
Operational readiness shall cover application support, infrastructure support, integration support, cybersecurity, data management, monitoring, backup and recovery, incident management and service management.

2.2.5.16.3 Handover to KPC

The Contractor shall progressively hand over operational responsibilities to designated KPC personnel.

The handover shall include the transfer of relevant system knowledge, configurations, documentation, operational procedures, support records, known issues, licences, credentials where applicable and other information required for effective operation of the Solution.

2.2.5.16.4 Support Transition

The Contractor shall provide appropriate support during the transition period and shall ensure that there is no interruption to business operations as responsibilities move from the implementation team to the agreed steady-state support arrangement.

The Contractor shall remain responsible for unresolved implementation defects and outstanding contractual obligations during the transition.

2.2.5.16.5 Operational Procedures

The Contractor shall provide and validate operational procedures covering routine system administration, monitoring, incident management, problem management, change management, backup and recovery, security management, performance management and escalation.

2.2.5.16.6 Final Transition Assessment

The Contractor shall undertake a formal transition assessment to confirm that the agreed transition requirements have been satisfied.

The assessment shall identify any remaining gaps, risks, dependencies or outstanding activities and shall include an agreed action plan for their resolution.

2.2.5.16.7 Transition Completion

Transition to business-as-usual operations shall be completed only after KPC confirms that the required operational capabilities, documentation, knowledge transfer, support arrangements and contractual obligations have been satisfactorily completed.

Completion of transition shall not relieve the Contractor of its warranty, support, maintenance or other continuing contractual obligations.

2.2.5.17 *Continuous Improvement and Technology Evolution*

The Contractor shall support KPC in continuously improving the Enterprise Digital Transformation Solution throughout the Contract and applicable support period.

2.2.5.17.1 Continuous Improvement

The Contractor shall identify opportunities to improve system performance, business process efficiency, automation, user experience, data quality, integration, security and operational effectiveness.

Improvement recommendations shall be based on system performance, user feedback, incident trends, business requirements, technology developments and other relevant information.

2.2.5.17.2 Business Process Optimisation

The Contractor shall support KPC in identifying opportunities to simplify, automate and optimise implemented business processes.

Proposed process improvements shall be assessed for their impact on approved business processes, controls, integrations, data, security and Solution Architecture before implementation.

2.2.5.17.3 Technology Updates

The Contractor shall keep KPC informed of significant developments, product releases, security updates, technology lifecycle changes and other developments affecting the Solution.

The Contractor shall recommend appropriate upgrades or enhancements where they provide material benefits to KPC.

2.2.5.17.4 Product Upgrades

The Contractor shall support the assessment, planning, testing and implementation of approved product upgrades and technology updates.

Upgrades shall be managed through KPC's approved change and release management processes and shall preserve existing approved functionality, integrations, security controls and data integrity.

2.2.5.17.5 Emerging Technologies

Where appropriate, the Contractor shall advise KPC on relevant emerging technologies, including Artificial Intelligence, Machine Learning, intelligent automation, advanced analytics, process automation, mobile technologies and other digital capabilities that may enhance the Solution.
Implementation of any emerging technology shall be subject to KPC's approval and applicable security, data protection, governance and commercial requirements.

2.2.5.17.6 Performance Improvement

The Contractor shall periodically review the performance, capacity, availability and reliability of the Solution and recommend optimisation measures where required.
Performance improvement activities shall address recurring incidents, system bottlenecks, capacity constraints, inefficient configurations and other identified sources of performance degradation.

2.2.5.17.7 Security Improvement

The Contractor shall continuously assess the Solution for emerging cybersecurity risks, vulnerabilities and applicable security developments.
The Contractor shall recommend and implement approved security improvements, patches, configuration changes and other measures necessary to maintain the security posture of the Solution.

2.2.5.17.8 Continuous Improvement Reporting

The Contractor shall provide periodic reports identifying recommended improvements, their expected benefits, implementation priorities, dependencies, risks and estimated resource or cost implications.
KPC shall determine which improvements are to be implemented through the applicable governance and change control processes.

2.2.5.17.9 Sustainability

All improvements and technology changes shall preserve the maintainability, scalability, interoperability, security and long-term sustainability of the Enterprise Digital Transformation Solution.
The Contractor shall avoid introducing technologies or configurations that create unnecessary vendor lock-in, unsupported dependencies or material barriers to future enhancement of the Solution.

2.2.5.18 *General Contractor Responsibilities*

The Contractor shall have overall responsibility for the successful delivery, integration, commissioning, operation and support of the Enterprise Digital Transformation Solution in accordance with the requirements of this TENDER and the Contract.

2.2.5.18.1 End-to-End Responsibility

The Contractor shall be responsible for coordinating and delivering all components, activities and dependencies necessary to achieve a complete, integrated and operational Solution.
The Contractor shall not limit its responsibility to individual products, applications, infrastructure components or services where successful operation requires coordination between multiple components.

2.2.5.18.2 Coordination of OEMs and Subcontractors

Where OEMs, subcontractors, consortium members or other third parties are engaged, the Contractor shall remain fully responsible for coordinating their activities and ensuring compliance with the Contract.
The Contractor shall ensure that all third-party activities are integrated into the overall implementation plan, testing programme, documentation, knowledge transfer and support arrangements.

2.2.5.18.3 Solution Dependencies

The Contractor shall identify all technical, functional, infrastructure, licensing, integration, data, security and operational dependencies required for successful implementation and operation of the Solution.

All identified dependencies shall be documented and included in the relevant implementation plans and Bill of Materials.

2.2.5.18.4 Completeness of the Solution

The Contractor shall provide all components necessary to deliver a complete and operational Solution, whether or not each component is expressly identified in the TENDER.

Any component, licence, interface, integration, infrastructure element, configuration, development, professional service or other requirement necessary to achieve the specified functionality and performance shall be deemed included in the Contractor's scope.

2.2.5.18.5 Compliance with Approved Designs

The Contractor shall implement the Solution in accordance with the approved architecture, designs, To-Be processes, specifications, implementation plans and applicable KPC standards.

Any proposed deviation shall be documented and submitted to KPC for approval before implementation.

2.2.5.18.6 Quality Assurance

The Contractor shall maintain appropriate quality assurance processes throughout the implementation and support lifecycle.

The Contractor shall ensure that all deliverables, configurations, developments, integrations, documentation and services are subject to appropriate quality control and verification before submission to KPC.

2.2.5.18.7 Resource Requirements

The Contractor shall provide suitably qualified and experienced personnel in sufficient numbers to undertake the required activities and meet the approved implementation schedule.

The Contractor shall ensure continuity of key personnel throughout critical implementation stages and shall obtain KPC approval for replacement of designated key personnel where required under the Contract.

2.2.5.18.8 Risk Management

The Contractor shall proactively identify, assess, monitor and manage risks affecting delivery of the Solution.

Risks relating to scope, schedule, technology, integration, data migration, infrastructure, cybersecurity, OT integration, resources, quality and business readiness shall be continuously monitored and reported to KPC.

2.2.5.18.9 Business Continuity During Implementation

The Contractor shall plan and execute implementation activities in a manner that minimises disruption to KPC's ongoing business and operational activities.

Where implementation activities may affect production systems or critical operations, the Contractor shall obtain the required approvals and implement appropriate contingency and rollback arrangements.

2.2.5.18.10 Regulatory and Policy Compliance

The Contractor shall comply with all applicable Kenyan laws, regulations, standards and KPC policies relevant to the delivery and operation of the Solution.

The Contractor shall ensure that all proposed technologies, processes, integrations and services are implemented in accordance with applicable regulatory, security, data protection, records management and operational requirements.

2.2.5.18.11 Intellectual Property and Use of Deliverables

The Contractor shall provide KPC with the rights, licences and documentation necessary to use, operate, maintain and support all deliverables provided under the Contract in accordance with the applicable contractual terms.

For custom developments undertaken specifically for KPC, the ownership and usage rights shall be governed by the applicable provisions of the Contract.

2.2.5.18.12 Confidentiality and Protection of KPC Information

The Contractor shall protect all KPC information, data, documents, system configurations, credentials, technical information and other confidential information accessed or processed during implementation and support.
Such information shall only be accessed, processed, copied, transferred or disclosed for authorised purposes and in accordance with the Contract and applicable KPC security requirements.

2.2.5.18.13 Contractor Accountability

The Contractor shall remain accountable for the overall quality, completeness, interoperability, security, performance and supportability of the Enterprise Digital Transformation Solution throughout the implementation, warranty and applicable support periods.
Acceptance of individual components or deliverables by KPC shall not relieve the Contractor of its responsibility to ensure that the complete Solution operates as an integrated and functional enterprise environment.

2.2.6 Bill of Materials (BOM)

2.2.6.1 *General BOM Requirements*

The Tenderer shall provide a complete, itemised and fully reconciled Bill of Materials (BOM) covering all software, licences, subscriptions, infrastructure, databases, middleware, integrations, implementation services, data migration, training, change management, support, maintenance and any other components required to deliver, commission, operate and support the Enterprise Digital Transformation Solution.

i. The BOM shall be aligned with the technical and functional requirements specified in this Section and shall provide sufficient detail to enable KPC to evaluate the proposed solution, compare commercial proposals and determine the Total Cost of Ownership (TCO).
ii. The Tenderer shall identify the proposed product, OEM, licensing or pricing metric, quantity, one-time cost, recurring cost and total contract cost for each applicable item.
iii. All third-party products, OEM licences, cloud services, subscriptions, connectors, APIs, middleware, development tools, security components and other externally licensed or supplied components required for the proposed Solution shall be identified, itemised and priced.
iv. The BOM shall form part of the Contract and shall constitute the basis for establishing the Contractor's obligations regarding the supply, implementation, licensing, configuration, integration, support and maintenance of the Solution.
v. The Tenderer shall ensure that all dependencies and prerequisites necessary for the complete operation of the proposed Solution are included in the relevant BOM. Any other component necessary for the successful delivery, integration, performance, security, operation or support of the Solution but omitted from the BOM shall be deemed included in the Contract Price.
vi. The Tenderer shall clearly distinguish between one-time costs and recurring costs and shall identify the applicable licensing or pricing model, including Named User, Concurrent User, Enterprise Licence, Subscription, Consumption-Based or any other applicable metric.
vii. The Tenderer shall identify all annual recurring costs, including software assurance, licence renewals, subscriptions, OEM support, infrastructure support, database support, cybersecurity support, cloud services and managed services, where applicable.
viii. The BOM shall cover the full implementation and support period specified in the tender and shall provide sufficient information to determine the financial impact of recurring costs throughout the Contract period.
ix. The Tenderer shall not exclude any required component necessary for the successful delivery, integration, performance, security, operation or support of the Solution on the basis that it is a prerequisite, supporting component or third-party dependency. All such components shall be identified and priced.
x. The Tenderer shall ensure that the detailed BOM reconciles fully with the Commercial Summary.
xi. The Tenderer shall identify the specific licensing metric applicable to each proposed product.
xii. Where a capability is provided as part of another proposed product without a separate licence, the Tenderer shall indicate **"Included"** and identify the parent product.
xiii. The contract award shall be for three (3) years renewable once at the same price. Subscription and support pricing shall be **fixed for the initial term of Six (6) years from first Production Go-Live,** applicable to the KPC's then-current quantities.
xiv. For the legacy ERP system replacement proposal, a greenfield implementation approach shall be used.

2.2.6.2 *Solution Sizing Information*

2.2.6.2.1 Enterprise-Wide Parameters

Parameters in this section drive sizing across every layer of the solution. They shall be treated as the master volumetric baseline; layer-specific parameters below inherit from them.

Ref	Parameter	Unit / Format	KPC Value
A1	Legal entities and company structure	Count + organisation chart	1 legal entity, 26 business units and 3 profit centres.
A2	Physical sites in scope: HQ, pump stations, depots, terminals, jetty facilities	Count + site list with locations	KPC Head Office, 54 pump stations/plants, 7 inland loading terminals, 2 marine discharge terminals, 3 marine loading terminals, 2 aviation terminals, 6 warehouses and other approved operational facilities.
A3	Total headcount by category (management, technical, field, operational, casual)	Count per category	Approximately 1,500 employees in total. Executive – 11 Management – 38
A4	Named users vs peak concurrent users, by role persona	Count + concurrency %	Named ERP users - 1000 Named HR only users – 500 Peak Users - 500
A5	Shift pattern and 24/7 operations coverage	Description	KPC operates critical operational facilities on a 24/7 basis. 5 Shifts in KPC
A6	Growth assumption over the contract term	% per annum + term (base + extension years)	The solution shall support growth throughout the contract period. The contract award shall be for three (3) years, renewable once. Subscription and support pricing shall remain fixed for six (6) years from the first Production Go-Live, based on KPC's then-current quantities. 11% growth per annum
A7	Currencies, languages and fiscal calendar	List	US Dollar and Kenyan Shilling (KES) are the

Ref	Parameter	Unit / Format	KPC Value
			primary operating currencies, with support for other approved currencies; English as the primary business language; and the KPC-approved fiscal calendar is July 1st to June 30th
A8	Data residency and Data Protection Act 2019 constraints	Policy statement	The solution shall comply with the Kenya Data Protection Act, 2019, applicable Critical Information Infrastructure Protection guidelines, and KPC data governance, cybersecurity and regulatory requirements.

2.2.6.2.2 Application Layer: ERP

Ref	Parameter	Unit / Format	KPC Value
B1	Module scope confirmation (Finance, SCM, EAM, Projects; HCM boundary with E-HR/ESS)	Scope / RACI matrix	27
B2	User counts by Current ERP licence class (full, limited, mobile maintenance, self-service)	Count per class	Business Suite Ltd Professional — 67 Business Suite Professional — 591 Payroll Processing — 6 Oracle DB — 1 Enterprise Support — 1 Business Suite Professional — 5 Business Suite Ltd Professional — 133 Oracle DB — 1 Enterprise Support — 1 BusObj Mobile (USR) — 20 Application Business Analyst User — 5 BusObj BI starter package — 1 Oracle DB — 1 Enterprise Supp. f. BusObj portfolio — 1 Mobile Platform — 150 Employee Self-Service User — 1500 WPB Enterprise Edition — 296 Ent Int-Work Manager MobApp — 20 Ent Int-Leave Request

Ref	Parameter	Unit / Format	KPC Value
			MobApp — 150 ASE Runtime Edition — 1 Appl. Ltd.Prof. Upgr. User (from BI) — 66 Manuf. Integr. + Intell. (MII) — 2 Sybase Unwired Platform Ent. Developer — 5 Sybase IQ Enterprise Edition — 2 Ent Int-Mobile Workflow MobApp — 150 Hydrocarbon Supply&Primary Distr O&G — 4 Manager Self-Service User — 316 WPB Producer — 2 Enterprise Support — 1 Enterprise Support for Sybase — 1 Logistics User — 907 Worker User — 266/329 ASE Runtime Edition — 1 Enterprise Support for Sybase — 1 Enterprise Support — 1 Extended Sourcing — 100 Spend Performance Management — 200 Supplier Lifecycle Management — 400 Extended Procurement — 100 Contract Lifecycle Mgmt (CLM) — 5 Oracle DB — 1 Enterprise Support — 1 Process Integration/Orchestration — 4 Enterprise Support — 1 ASE Runtime Edition — 1 Enterprise Support for Sybase — 1 Developer User — 3 Single Sign-On — 7 Access Control — 18 ASE Runtime Edition — 1
B3	Maintainable asset register: functional locations and equipment objects (pipeline segments, pumps, tanks, valves, instruments, fleet)	Counts by asset class	81784
B4	Work orders per month (corrective + preventive) and active PM plans	Count	1688

Ref	Parameter	Unit / Format	KPC Value
B5	Inventory: stock items (SKUs), storerooms/warehouses, issue/receipt transactions per day	Counts	13331
B6	Financial volumes: GL journal lines p.a., AP invoices p.a., AR invoices p.a., fixed asset records	Counts	Fixed Assets 173,676 GL Journal Line 556,906, AP 33,977 AR 131,859
B7	Capital projects: active projects and WBS depth	Count + levels	1348 projects
B8	Legacy SAP migration: history years, object list, data volume	Years + GB + object counts	ECC 6 - 20 years – 15.5TB
B10	Environments required (PRD, DR, QA, DEV, TRN) and refresh frequency	Environment matrix	4
B11	Availability, RPO and RTO targets for ERP tier	% + hours	99.9% Availability, RTO 2hrs RPO 30 mins
B12	Reporting: operational reports, statutory reports, dashboards, analytics users	Counts	10 Dashboards, 1000 Reports

2.2.6.2.3 Application Layer : E-Procurement (SaaS)

Ref	Parameter	Unit / Format	KPC Value
C1	Annual addressable spend under management	KES (bn)	KES 5 billion
C2	Active suppliers and expected new registrations per annum	Counts	2300 awarded suppliers, 16,000 total registered suppliers; estimate 200–300 supplier registrations/year
C3	Requisitions, purchase orders and invoices per annum	Counts	1000 Requisitions; 500Purchase Orders; 400 Invoices per annum
C4	Sourcing events per annum by KPC procurement methods (open tender, restricted, RFQ, framework, direct)	Count per method	Open Tender: 126; Restricted: 41; RFQ: 146; Framework: 10; Direct: 23
C5	Contracts under management and renewals per annum	Counts	150 Contracts; 20 Renewals per annum
C6	Requesters / approvers (self-service population) vs procurement power users	Counts	800 Self-Service Requesters/Approvers; 50 Procurement Power Users
C7	Catalogues and supplier punchouts planned	Count	Product Catalog, Service catalog
C8	Approval workflow complexity: delegation-of-authority levels	DoA matrix	Upto 6 Delegation-of-Authority Approval Levels

Ref	Parameter	Unit / Format	KPC Value
C9	Statutory integrations: KRA eTIMS e-invoicing; any publication obligations	Requirement statement	KRA eTIMS/e-Invoicing Integration;
C10	Integration flows to ERP (PO, goods receipt, invoice, supplier master, budget check)	Interface list	Upto 10 Integration Interfaces: Supplier Master, Requisition, Goods Receipt, Invoice, Budget Check, Contract Data, Chart of Accounts/Cost Centres, Material/Service Master and Payment Status

2.2.6.2.4 Application Layer: HCM/Finance Integration Boundary

Ref	Parameter	Unit / Format	KPC Value / Mandated Assumption
D1	Employee records mastered in e-hr and sync scope to ERP and E-procurement	Count + attribute list	1,500
D2	Functional boundary statement: which finance/HCM processes may remain in E-HR	Boundary matrix	Workforce Planning and Establishment Management Recruitment and Onboarding Employee Administration Time, Attendance and Leave Management Payroll and Benefits Management Performance, Learning and Talent Management Employee and Manager Self-Service HR Governance and Compliance HR Reporting and Workforce Analytics Integration and Governance
D3	Interface flows e-hr ↔ erp ↔ e-procurement (cost centres, GL postings, worker data, approvals)	Interface list with frequency	One Identity and AD is the identity source of truth; SSO shall be supported using SAML 2.0 and/or OpenID Connect (OIDC), as applicable.
D4	Identity source of truth and SSO standard (e.g. Entra ID / SAML / OIDC)	Statement	Consolidated HCM/Finance management reporting required; detailed report inventory and volumes.
D5	Cross-platform reporting obligations (consolidated management reporting)	Report list	Time, Attendance and Leave Management

2.2.6.2.5 MSOOS

Ref	Parameter	Unit / Format	KPC Value / Mandated Assumption
E1	Pipeline network: line lengths, diameters, products	km + line list	Line 5 – 450 km, 20” Line 2 – 325 km, 8”/6” Line 4 – 325 km, 14” Line 3 – 121 km, 6”

<table>
<tr><th>Ref</th><th>Parameter</th><th>Unit / Format</th><th>KPC Value / Mandated Assumption</th></tr>
<tr><td></td><td>carried, elevation profile availability</td><td></td><td>Line 6 – 121 km, 10”
Multi Product Pipeline</td></tr>
<tr><td>E2</td><td>Pump stations and delivery/receipt points</td><td>Counts</td><td>Pump stations - 21
Delivery Points - 9
Receipt points - 4</td></tr>
<tr><td>E8</td><td>Terminals/depots in scope; per depot: loading bays, arms, meters, flow computers, truck loadings per day</td><td>Counts per depot</td><td>
<table>
<tr><th>Terminal</th><th>Loading Bays</th><th>Arms</th><th>Meters</th><th>Flow Computers</th><th>truck loading per day</th></tr>
<tr><td>PS09</td><td>2</td><td>2</td><td>2</td><td>1</td><td>16</td></tr>
<tr><td>PS10</td><td>6</td><td>12</td><td>12</td><td>6</td><td>Approx. 200</td></tr>
<tr><td>PS25</td><td>6</td><td>12</td><td>12</td><td>5</td><td>714</td></tr>
<tr><td>PS27</td><td>12</td><td>22</td><td>22</td><td>8</td><td>912</td></tr>
<tr><td>PS28</td><td>10</td><td>27</td><td>27</td><td>15</td><td>706</td></tr>
</table>
PS09 – Hydrant Pits – 126</td></tr>
<tr><td>E9</td><td>Batch operations: batches per month, tank count and capacities, interface volumes</td><td>Counts + m³</td><td>Batches per month
Line 5 – 18
Line 4/6 – 9
Tank count and capacities
Tanks – 164
Capacity - 1,073,000M3</td></tr>
<tr><td>E10</td><td>Shippers/OMCs served and nominations per cycle</td><td>Counts</td><td>OMCs - 232, Active -160, In active - 72
nominations per cycle Avg 88796 per month</td></tr>
<tr><td>E11</td><td>O2C volumes: ullage transactions, allocations, shipper invoices per month; KRA-ICMS interface specification</td><td>Counts + interface spec</td><td>O2C volumes - 884282.56M3 Avg. per month
Shipper invoices per month - Avg 1018 per month
KRA-ICMS interface specification - SOAP/XML web service (iCMSService), with Action identifying the transaction and RequestMsg carrying the XML business payload in CDATA.
KRA-TIMS interface specification - RESTful web service using HTTP POST, transmitting invoice data in JSON format,</td></tr>
<tr><td>E14</td><td>Redundancy requirements per layer</td><td>Requirement statement</td><td>The proposed solution shall provide appropriate redundancy and high-availability capabilities across all applicable infrastructure, application, database, integration, network and security layers to eliminate single points of failure for critical services.</td></tr>
</table>

2.2.6.2.6 Data & Analytics / ML Layer

Ref	Parameter	Unit / Format	KPC Value
H1	Source systems in analytics scope	System list	ERP, MSOOS, SCADA, TMS, e-Procurement, e-HR and other approved internal and external source systems. Additional source systems may be integrated during the contract period.
H2	Estimated analytical data volume and annual growth	TB and TB per annum	5 TB initial analytical data volume with an estimated annual growth of 10%
H3	Data refresh latency requirements by subject area	Latency per subject area	Daily batch processing as the standard requirement, with near-real-time or real-time integration for approved operational use cases
H4	Dashboard and report inventory to be delivered at go-live	Number of dashboards and reports by complexity	Tenderer to propose and validate the detailed inventory during the requirements and design phase; solution shall support enterprise-scale dashboards and reports
H5	Analytics user tiers	Number of users by category	50 analytical users, including approximately 10 Data Engineers/Analysts and 5 Data Scientists
H6	ML/AI use cases within scope	Number and description of use cases	5 priority Enterprise Data Analytics & AI use cases, including predictive maintenance, demand forecasting, line performance analytics, operational optimisation, and revenue and throughput analytics.

2.2.6.2.7 Integration & Middleware Layer

Ref	Parameter	Unit / Format	KPC Value
I1	Full interface catalogue across the stack (ERP ↔ e-procurement ↔ MSOOS ↔ E-Hr ↔ KRA ↔ banks ↔ EDRMS)	Numbered list: direction, frequency, volume	ERP ↔ e-procurement ERP ↔ MSOOS ERP ↔ E-Hr ERP ↔ KRA ERP ↔ EDRMS ERP ↔ Banks 6No. MSOOS ↔ KRA MSOOS ↔SCADA MSOOS ↔ ATG MSOOS ↔ TMS
I2	Message volumes per day and peak transactions per second	Counts + TPS	6,774 messages per day Peak – 6 transactions per second (TPS)

Ref	Parameter	Unit / Format	KPC Value
I3	API consumers (internal apps, partner/regulator endpoints)	Counts	e-procurement MSOOS E-Hr KRA EDRMS Banks
I4	File-based vs API/event split and legacy protocols to support	Ratio + protocol list	6 Banks 6 Integrations
I5	Master data governance model (owners per domain: supplier, item, asset, employee, customer)	Governance matrix	Domain owner/steward for supplier, item, asset, employee, customer, etc.; system of record and golden-record authority
I6	Integration monitoring, alerting and replay requirements	Requirement statement	Monitoring coverage, alert thresholds, retry/replay rules, reconciliation requirements, retention period and operational SLA

2.2.6.2.8 Infrastructure Layer: Compute & Platform

<table>
<tr><th>Ref</th><th>Parameter</th><th>Unit / Format</th><th>KPC Value</th></tr>
<tr><td>J6</td><td>Primary data centre and DR data centre locations and separation</td><td>Sites + km</td><td>Primary Data Center at KPC Premises in Nairobi.
DR Data Center at Konza.

The two facilities are 79 Kilometers apart</td></tr>
<tr><td>J7</td><td>Environment matrix across all layers (PRD/DR/QA/DEV/TRN) with sizing ratio to production</td><td>Matrix + %</td><td>
<table>
<tr><th>Environment</th><th>Use</th><th>Ratio</th><th>Performance</th><th>High Availability</th></tr>
<tr><td>Production</td><td>Live System</td><td>100 %</td><td>Full scale peak load capacity</td><td>Clustered in Primary site

Warm Standby in DR</td></tr>
<tr><td>DR</td><td>Business Continuity</td><td>60%</td><td>Medium</td><td>Same as PRD architecture</td></tr>
<tr><td>Training</td><td>User on-boarding</td><td>40%</td><td>Medium</td><td>Backup</td></tr>
<tr><td>Quality</td><td>UAT</td><td>40%</td><td>Medium</td><td>Backup</td></tr>
<tr><td>Development</td><td>Code writing configurations</td><td>25%</td><td>Medium</td><td>Backup</td></tr>
</table>
</td></tr>
</table>

2.2.6.2.9 Infrastructure Layer: Storage & Backup

<table>
<tr><th>Ref</th><th>Parameter</th><th>Unit / Format</th><th>KPC Value</th></tr>
<tr><td>K1</td><td>Usable storage capacity required by tier (performance, capacity, archive)</td><td>TB per tier</td><td>
<table>
<tr><th>Tier</th><th>% usable Capacity</th><th>workload</th></tr>
<tr><td>NVME/SSD</td><td>25%</td><td>• Active production databases
• Boot disks
• Transactional data
• Real time analytics</td></tr>
<tr><td>SAS</td><td>40 %</td><td>• File shares
• Virtual Machines disks</td></tr>
<tr><td>NL-SASA</td><td>35%</td><td>• Long term Backup
• Historical logs
• Archives</td></tr>
</table>
</td></tr>
<tr><td>K2</td><td>IOPS and latency targets for database tiers</td><td>IOPS + ms</td><td>10,000 - 64,000+ IOPS</td></tr>
<tr><td>K3</td><td>Data growth rate across the estate</td><td>% or TB per annum</td><td>11% per annum</td></tr>
<tr><td>K4</td><td>Backup retention policy (operational, monthly, annual) and immutability requirement</td><td>Schedule + statement</td><td>Weekly full backup (every Saturday). Incremental backup every two hours.

7 years backup retention</td></tr>
<tr><td>K5</td><td>Archival policy and statutory retention obligations</td><td>Years by record type</td><td>7 years backup retention

Data on both tape and disk media</td></tr>
</table>

2.2.6.2.10 Infrastructure Layer: Network & Connectivity

Ref	Parameter	Unit / Format	KPC Value
L1	WAN links per station/depot: medium, bandwidth, availability, provider diversity	Site table	2
L2	Fibre availability along pipeline right-of-way	Route description	yes
L3	LAN/wireless refresh scope per site	Site list + counts	N/A
L4	Inter-DC bandwidth and latency (primary ↔ DR)	Mbps + ms	10Gigabit per Second 2 ms
L5	Internet breakout, DIA capacity and redundancy	Mbps + design	500mbps primary redundancy 200mbps
L6	Latency targets user-to-application per site class	ms	6 – 10 ms

2.2.6.2.11 Security Layer: IT & OT

Ref	Parameter	Unit / Format	KPC Value
M1	SIEM ingestion baseline (events per second / GB per day) and log source count	EPS + sources	250 GB/day 500Gb/per for future growth planning 5,000 sustained / 10,000 peak EPS and 250 GB/day
M2	Endpoint population for EDR (servers, workstations, OT-adjacent)	Counts	2000
M3	Privileged accounts and PAM user population	Counts	30
M4	IAM identities (staff, contractors, suppliers, service accounts) and lifecycle volumes	Counts	2500

2.2.6.2.12 End-User Computing Layer

Ref	Parameter	Unit / Format	KPC Value
N1	Device population by type	Counts	40 ATEX Mobile tablets
N2	Peripheral and specialist device scope	Counts	
N3	Productivity platform boundary	Boundary statement	Existing enterprise productivity and collaboration platforms shall remain under KPC management unless specifically included in the Tender scope. The Tenderer shall clearly identify all dependencies, integration requirements and any additional licences required for the proposed solution.

2.2.6.2.13 Facilities Layer: Data Centres

Ref	Parameter	Unit / Format	KPC Value
O1	DC rack space, power and cooling capacity available (primary and DR)	Racks + kW	**Primary DC:** 12-rack containerized data centre. Available Power Capacity: 200kW Available cooling capacity: **4 × 36,000 BTU (144,000 BTU total)**. Available rack space and power capacity to be confirmed during tenderer site survey. **DR Site:** Managed co-location facility with 2 × 42U racks including power and cooling services.
O2	UPS and generator autonomy at each hosting site	Minutes/hours	**Primary DC:** 2 × 60 kW UPS systems operating in redundant configuration. Generator-backed facility. UPS Autonomy: 750 min

Ref	Parameter	Unit / Format	KPC Value
			Generator Autonomy: 8 hours **DR Site:** UPS and generator services provided under the managed co-location service provider SLA.

2.2.6.2.14 Non-Functional Requirements & Service Levels

Ref	Parameter	Unit / Format	KPC Value
P1	Availability targets per service tier (OT, ERP, procurement, analytics, EDRMS)	% per tier	Tier 1 (ERP, MSOOS Procurement): 99.95%; Tier 2 (Analytics, Reporting): 99.90%; Tier 3 (Non-critical services): 99.50%
P2	RPO / RTO per service tier	Hours per tier	RPO ≤ 30 min, RTO ≤ 2 hrs
P3	Performance targets (screen response, batch windows, close cycle, loading authorisation time)	Quantified targets	As per Technical Performance Benchmarks
P4	Capacity headroom policy at go-live	% above Year-1 volumes	30% infrastructure and database capacity headroom above Year-1 forecast volumes
P5	Service desk and support model: hours, languages, priority matrix	SLA table	24x7 support for P1 incidents; 8x5 support for standard issues; English support; P1 Response: 15 min / Restore: 4 hrs; P2 Response: 30 min / Restore: 8 hrs; P3 Response: 4 hrs / Restore: 3 business days; P4 Response: 1 business day
P6	Hypercare duration and exit criteria	Weeks + criteria	6 Months Hypercare post Go-live (per release); Exit criteria: ≥99% critical defect closure, SLA achievement ≥95% for 4 consecutive weeks, successful knowledge transfer, business sign-off

2.2.6.2.15 Training, Change & Adoption

<table>
<tr><th>Ref</th><th>Parameter</th><th>Unit / Format</th><th>KPC Value</th></tr>
<tr><td>Q1</td><td>Training population by role and by site</td><td>Counts</td><td>Super users 50 No
End users 1500 No
Training Population by Role and Site highlighted below

<table>
<tr><th></th><th>Sites</th><th>Staff Count</th><th>Super Users</th><th>End users</th></tr>
<tr><td>1</td><td>PS 10 – Nairobi Terminal</td><td>361</td><td>11</td><td>350</td></tr>
<tr><td>2</td><td>Kenpipe Plaza</td><td>262</td><td>15</td><td>247</td></tr>
<tr><td>3</td><td>Ps 9 – Embakasi Depot</td><td>67</td><td>2</td><td>65</td></tr>
<tr><td>4</td><td>PS 14- Kipevu Oil Storage Facility Depot</td><td>95</td><td>2</td><td>93</td></tr>
<tr><td>5</td><td>PS 1 – Mombasa Depot</td><td>83</td><td>3</td><td>80</td></tr>
<tr><td>6</td><td>PS 12 – Mombasa International Airport</td><td>32</td><td>3</td><td>29</td></tr>
<tr><td>7</td><td>PS 25 – Nakuru Terminal</td><td>182</td><td>3</td><td>179</td></tr>
<tr><td>8</td><td>PS 27- Eldoret Terminal</td><td>134</td><td>2</td><td>132</td></tr>
<tr><td>9</td><td>PS 28 – Kisumu Terminal</td><td>149</td><td>3</td><td>146</td></tr>
<tr><td>10</td><td>PS15 – KPRL</td><td>115</td><td>3</td><td>112</td></tr>
<tr><td>11</td><td>KOT2 – Kipevu oil Terminal</td><td>20</td><td>3</td><td>17</td></tr>
<tr><td></td><td>Total</td><td>1500</td><td>50</td><td>1450</td></tr>
</table>
</td></tr>
<tr><td>Q1 B</td><td>Stakeholder Training</td><td>Count</td><td>• 1000 Customers
• 3000 Suppliers
• 3000 Drivers</td></tr>
<tr><td>Q2</td><td>Training delivery constraints</td><td>Statement</td><td>• We recommend training delivery to include Classroom, virtual, hybrid, or hands-on training depending on the module
• Shift Release: Staff will be released in staggered groups to ensure business continuity
• Classroom Capacity: Maximum participants (20 No.) per session based on room size</td></tr>
<tr><td>Q3</td><td>Training delivery model</td><td>Statement</td><td>• Train the Trainer delivery method-we expect the 50 No. Super Users to be trained first to support end-user training and post-go-live support
• Direct delivery method- We expect the 1450 No. End users to be trained using direct delivery model</td></tr>
<tr><td>Q4</td><td>Training environments and refresh cadence</td><td>Count and cadence</td><td>• We expect the 1500 No. Users to undergo initial training before go-live
• Refresh cadence -To drive adoption and maintain knowledge and skills, we recommend Refresher training after 6 months and annual refresher training thereafter</td></tr>
<tr><td>Q5</td><td>Change network: champions</td><td>Counts</td><td>• We expect 75 No. Champions to drive the change and adoption of the solution. Ratio proposed: 1 champion for 20 users</td></tr>
</table>

	and super users per department/ site		`	**Sites**	**Staff Count**	**Champions**
			1	PS 10 – Nairobi Terminal	361	18
			2	Kenpipe Plaza	262	15
			3	Ps 9 – Embakasi Depot	67	3
			4	PS 14- Kipevu Oil Storage Facility Depot	95	5
			5	PS 1 – Mombasa Depot	83	5
			6	PS 12 – Mombasa International Airport	32	5
			7	PS 25 – Nakuru Terminal	182	5
			8	PS 27- Eldoret Terminal	134	5
			9	PS 28 – Kisumu Terminal	149	5
			10	PS15 – KPRL	115	5
			11	KOT2 – Kipevu oil Terminal	20	5
				Total	**1500**	**75**

Enterprise Data Analytics & AI KPC Baselines

Parameter	Pricing Basis
Initial analytical data	5 TB
Growth	10% p.a.
Year 5 data	~7.3 TB
Analytical users	50
Data Engineers/Analysts	10
Data Scientists	5
Availability	24×7
Enterprise Data Analytics & AI use cases	5
ETL/ELT	Daily
Near-real-time integration	Required
Power BI	Existing
Primary environment	1
DR	1
Retention	5 years
GenAI	5M tokens/month
ML training	200 compute hours/month
GPU	100 GPU hours/month
Contract	5 years

The following are the Bill of materials that will inform both Technical and Financial submissions.

2.2.6.3 *Business Applications BOM*

No.	Business Application / Capability	Proposed OEM / Product	Licensing Metric	KPC Baseline Quantity
1.	Financial Operations		Users	300
2.	Supply Chain Management		Users	893
3.	Human Capital Management		Users	1,500
4.	Payroll		Payroll Load	1,500
5.	Enterprise Asset Management		Users	600
6.	Project Lifecycle Management		Users	200
7.	Strategic Planning and Performance Management		Users	100
8.	Enterprise Risk Management		Users	100
9.	Identity, access control, Multi-Factor and SSO		Users	1500
10.	Customer Relationship Management (CRM)		Users	100
11.	E - Procurement		Users	500
12.	Contract Lifecycle Management (CLM)		Users	100
13.	Sales and Commercial Management		Users	50
14.	Safety Management		Users	1500
15.	IT Service Management (ITSM)		Users	50
16.	Enterprise Monitoring and Observability		Users	30
17.	Integrated Development platform and workflow & Business Process Automation		Users(developers)	20

No.	Business Application / Capability	Proposed OEM / Product	Licensing Metric	KPC Baseline Quantity
18.	Integration platform		Integration Points	All Integration points
19.	Comprehensive instructor-led certification training for 60No staff Functional Superuser ERP training Solution at OEM's authorized training center that has been in operation for at least 5 years	60No LOT	LOT	
20.	Comprehensive instructor-led certification training for 15No. Technical users ERP training Solution at OEM's authorized training center that has been in operation for at least 5 years	15No LOT	LOT	
21.	Include any other component necessary for the solution to meet all the functional and technical requirements.		LOT	LOT
22.	Annual Maintenance if applicable		LOT	

2.2.6.4 ***Mid-Stream Oil Operations Solution and Terminal Management Solution BOM***

i. MSOOS will be centrally deployed while TMS will be deployed on the Terminals

ii. The Tenderer shall provide a complete and fully itemized Bill of Materials for the Terminal Management System (TMS), Queue Management, Truck Inspection, Driver and Vehicle Management, Loading Operations and Loading Automation solution.

iii. The BOM shall include all software, licences, terminal equipment, TMS-specific site infrastructure, interfaces, integration components, implementation services, training, warranty, support and other components required to provide a complete and operational solution across the approved KPC loading terminals.

iv. The TMS shall support the loading terminals identified in the Tender baseline: **PS09, PS10, PS25, PS27 and PS28. The MSOOS shall integrate to Honeywell TMS in KPRL, and COTAS in PS12.**

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity
1	**Order & Inventory Management**	Order management, inventory management, quantity conversion and standardisation	User / Enterprise	1 LOT	
2	**Nominations, Scheduling & Demand Forecasting**	Nominations, scheduling, allocation, capacity planning and demand forecasting	User / Enterprise	1 LOT	
3	**Terminal Management**	Terminal operations, truck/driver management, loading operations, loading station/arm management, gate and queue management	Terminal / Loading Station	1 LOT	
4	**Quality Control Management**	Product quality management, inspection, quality records and certificates	User / Enterprise	1 LOT	
5	**MSOOS Certification Training**	Comprehensive instructor-led certification training on 20No MSOOS Solution at OEM's authorized training center that has been in operation for atleast 5 years	Pax	20No	
6	**Other Required Components**	Any additional licences, modules, interfaces, middleware, software or services required for a complete solution	LOT	1	

2.2.6.5 *Enterprise Data Analytics & AI BOM*

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity
1	**Enterprise Data Analytics Platform**	Cloud data lake/Lakehouse, analytical platform, storage and processing capacity for 5 TB initial data with 10% annual growth	Subscription / Consumption	**1 LOT**	
2	**Data Integration & Data Engineering Platform**	ETL/ELT, API, CDC, batch and near-real-time integration, orchestration and data quality	Subscription / Consumption	**1 LOT**	
3	**Enterprise AI, Machine Learning, Data Science & Generative AI Platform**	AI/ML, data science, model development and MLOps, predictive and prescriptive analytics, forecasting, anomaly detection, Generative AI, natural-language analytics, intelligent recommendations and AI-assisted decision support	Subscription / Consumption	**1 LOT**	
4	**Data Governance, Security & Metadata Management**	Data catalogue, metadata, lineage, data quality, access control, audit, privacy and AI/ML governance	Subscription / Consumption	**1 LOT**	
5	**Power BI Integration**	Integration with KPC's existing Power BI environment, semantic models, analytical datasets, AI outputs and governed reporting data	Integration / LOT	**1**	
6	**Enterprise Systems & External Data Integration**	Integration with ERP/Core System, TMS, EAM, HR, ITSM, operational systems, IoT/SCADA and approved external data sources	Integration / LOT	**1**	
7	**Cloud Infrastructure, HA, Backup & DR Services**	Compute, storage, network/data transfer, high availability, backup, disaster recovery, monitoring and security services	Subscription / Consumption	**1 LOT**	

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity
8	**Implementation, Deployment & Priority AI/Analytics Use Cases**	Requirements validation, detailed solution architecture, platform configuration, data integration, testing, commissioning, and development/deployment of 5 agreed priority AI and advanced analytics use cases	LOT	**1**	
9	**Analytics/ML Certification Training**	Comprehensive instructor-led certification training on 12No AI/ML and analytics training Development at OEM's authorized training center that has been in operation for atleast 5 years	Pax	12No	
10	**Knowledge Transfer**	Administration, data engineering, data science	Pax	**30No**	
11	**Support, Maintenance, Updates & Technical Assistance**	24×7 support, platform maintenance, software updates, security patches, upgrades and technical assistance	Annual Subscription	**5 Years**	
12	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**	

2.2.6.6 *Enterprise Middleware & Application Development Platform BOM*

No.	BOM Component	Description / Scope	License Metric	Estimated Qty.	Tenderer Proposed Quantity
1	**Integration Platform**	Core middleware / integration platform	Lot	**1**	
2	**API Management Platform**	API publishing, lifecycle management and governance	Lot	**1**	
3	**Enterprise Service Bus (ESB)**	Service orchestration and application integration	Lot	**1**	
4	**Message Broker**	Asynchronous messaging and event distribution	Lot	**1**	
5	**Event Streaming Platform**	Real-time event streaming and processing	Lot	**1**	

6	**Workflow / Orchestration Engine**	Process orchestration across systems	Lot	**1**	
7	**Data Transformation Engine**	Mapping, transformation and enrichment	Lot	**1**	
8	**Integrations and Application Development Certification**	Comprehensive instructor-led certification training on 15No Integrations and Application Development at OEM's authorized training center that has been in operation for atleast 5 years	Pax	15No	
9	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**	

2.2.6.7 *Infrastructure BOM*

The system sizing provided below is based on the projected requirements and should be treated as a baseline. The tenderer should undertake their own sizing based on all the provided information and offer infrastructure that can meet or exceed the stated performance metrics in SECTION IIA. Should the delivered infrastructure prove insufficient, at the time of Go-Live, to achieve the required Technical Performance Benchmarks, the tenderer shall provide additional resources and capacity enhancements at no extra cost to meet or exceed the stated system performance requirements.

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
ERP	Development	ERP App	3	4	3.0 GHz	12	64	192
	Test	ERP App	3	5	3.0 GHz	15	64	192
	UAT	ERP App	3	5	3.0 GHz	15	64	192
	Production	ERP App - App/Middleware	4	8	3.0 GHz	32	64	256
	Production	ERP App - Web Front-End	2	4	3.0 GHz	8	32	64

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
	Production	ERP App - Batch/Scheduler	2	4	3.0 GHz	8	32	64
	Development	ERP DB	1	8	3.0 GHz	8	256	256
	Test	ERP DB	1	8	3.0 GHz	8	256	256
	UAT	ERP DB	1	8	3.0 GHz	8	256	256
	Production	ERP DB - Active/Active	2	16	3.0 GHz	32	1024	2048
	Production	ERP DB - Read Replica	1	8	3.0 GHz	8	256	256
MSOOS	Development	O2C - Pipeline Operations Application Server	1	8	3.0 GHz	8	64	64
	Development	O2C - Central Scheduling Application Server	1	8	3.0 GHz	8	64	64
	Development	O2C - Central Scheduling Optimisation Engine	1	8	3.0 GHz	8	64	64
	Development	O2C - Database	1	8	3.0 GHz	8	64	64
	Test	O2C - Pipeline Operations Application Server	1	8	3.0 GHz	8	64	64
	Test	O2C - Central Scheduling Application Server	1	8	3.0 GHz	8	64	64
	Test	O2C - Central Scheduling Optimisation Engine	1	8	3.0 GHz	8	64	64

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
	Test	O2C - Database	1	8	3.0 GHz	8	64	64
	Production	O2C - Pipeline Operations Application Server	2	4	3.0 GHz	8	128	256
	Production	O2C - Central Scheduling Application Server	2	4	3.0 GHz	8	128	256
	Production	O2C - Central Scheduling Optimisation Engine	2	4	3.0 GHz	8	128	256
	Production	O2C - Database (Dedicated HA pair)	2	8	3.0 GHz	16	256	512
Integration Platform	Development	Integration Runtime Cluster	2	2	3.0 GHz	4	32	64
	Test	Integration Runtime Cluster	2	2	3.0 GHz	4	32	64
	Production	Integration Runtime Cluster	3	4	3.0 GHz	12	64	192
	Development	API Gateway / Message Broker	2	2	3.0 GHz	4	32	64
	Test	API Gateway / Message Broker	2	2	3.0 GHz	4	32	64
	Production	API Gateway / Message Broker	3	4	3.0 GHz	12	64	192
Cloud Gateway	Production	Cloud Data-Export Gateway	2	4	3.0 GHz	8	64	128
	Production	Management Server	2	64	3.0 GHz	128	128	256

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
Enterprise Analytics	Development	Standalone BI & Semantic Sandbox	1	8	3.0 GHz	8	32	32
	Test / UAT	Web Ingress / API Gateway	2	2	3.0 GHz	4	8	16
	Test / UAT	Semantic & Analytics App Server	2	8	3.0 GHz	16	32	64
	Test / UAT	Metadata & Caching DB	1	8	3.0 GHz	8	32	32
	Production	Web Ingress	2	4	3.0 GHz	8	16	32
	Production	Semantic Layer & BI App Server (HA)	4	16	3.0 GHz	64	64	256
	Production	In-Memory Query Cache	3	8	3.0 GHz	24	64	192
	Production	Metadata & Audit DB Cluster (HA)	2	16	3.0 GHz	32	64	128
	Production	Data Pipeline Orchestrator (Airflow)	2	8	3.0 GHz	16	32	64
E-HR	Production	Application Server	2	8	3.0 GHz	16	32	64
	Production	Web Server	2	4	3.0 GHz	8	16	32
	Production	Database Server	2	12	3.0 GHz	24	64	128
	Test/UAT	Application Server	1	8	3.0 GHz	8	16	16

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
	Test/UAT	Database Server	1	8	3.0 GHz	8	32	32
	Development	Application + DB Server	1	8	3.0 GHz	8	32	32
E-Procurement	**Development**	App & DB Single Node	1	8	3.0 GHz	8	32	32
	Development	Integration / API Sandbox	1	4	3.0 GHz	4	16	16
	Test / UAT	Web Dispatcher	2	2	3.0 GHz	4	8	16
	Test / UAT	Application Server	2	8	3.0 GHz	16	32	64
	Test / UAT	Database Server (Primary)	1	16	3.0 GHz	16	64	64
	Test / UAT	Integration / API Gateway	1	4	3.0 GHz	4	16	16
	Production	Web Dispatcher	2	4	3.0 GHz	8	16	32
	Production	Application Server	4	16	3.0 GHz	64	64	256
	Production	Database Server (HA Cluster)	2	32	3.0 GHz	64	256	512
	Production	Search / Analytics Node	2	8	3.0 GHz	16	32	64
	Production	Integration / API Gateway	2	8	3.0 GHz	16	32	64

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
Enterprise Monitoring	**Development**	Single-Node Server & DB	1	8	3.0 GHz	8	32	32
	Test / UAT	Web / Dashboard Interface	2	4	3.0 GHz	8	16	32
	Test / UAT	Monitoring Core Server	1	8	3.0 GHz	8	32	32
	Test / UAT	Time-Series Database	1	16	3.0 GHz	16	64	64
	Test / UAT	Distributed Collector Node	2	4	3.0 GHz	8	16	32
	Production	Web / UI & API Gateway	2	8	3.0 GHz	16	32	64
	Production	Monitoring Core Engine (HA)	2	16	3.0 GHz	32	64	128
	Production	Distributed Proxies / Collectors	4	8	3.0 GHz	32	32	128
	Production	Time-Series DB Cluster (Primary)	2	32	3.0 GHz	64	256	512
	Production	Log & Metric Indexer (Elastic)	3	16	3.0 GHz	48	64	192
Integrated Development Platform	**Development**	Single-Node IDP Sandbox	1	4	3.0 GHz	4	16	16
	Test / UAT	Single-Node IDP Staging	1	4	3.0 GHz	4	16	16
	Production	Ingress / API Gateway	1	2	3.0 GHz	2	4	4

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
	Production	Core IDP Engine & UI (Backstage)	1	4	3.0 GHz	4	16	16
	Production	GitOps Engine (ArgoCD / Flux)	1	4	3.0 GHz	4	16	16
	Production	Secret Mgmt & Vault	1	2	3.0 GHz	2	8	8
	Production	Metadata & Portal DB	1	4	3.0 GHz	4	16	16
	Production	Shared Artifact Registry	1	2	3.0 GHz	2	8	8
ITSM	**Development**	Standalone App & DB Single Node	1	4	3.0 GHz	4	16	16
	Test / UAT	Web Server	2	2	3.0 GHz	4	8	16
	Test / UAT	Application Server	1	8	3.0 GHz	8	24	24
	Test / UAT	Database Server	1	8	3.0 GHz	8	32	32
	Production	Web Server	2	4	3.0 GHz	8	16	32
	Production	Application Server (HA Cluster)	2	12	3.0 GHz	24	32	64
	Production	Database Server (Primary HA Cluster)	2	16	3.0 GHz	32	64	128
	Production	Search & Analytics Indexer	2	4	3.0 GHz	8	16	32

System	Landscape	Role	Qty	Cores/Node	Clock Speed	Total Cores	RAM/Node (GB)	Total RAM (GB)
	Production	API / Mail Gateway	2	4	3.0 GHz	8	16	32

2.2.6.7.1 Compute Platform

i. Compute Platform – Primary Site

Item	Description	Qty
1.	Enterprise x86 Rack Servers	6
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
6.	Comprehensive instructor-led certification training on operating system and security administration, virtualization, containerization, database and performance tuning Training for Proposed Compute Platform for 5No. System Administrators at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	5
7.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.	

ii. Compute Platform – DR Site

Item	Description	Qty
1.	Enterprise x86 Rack Servers	4
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
6.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.	

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements including performance metrics.
3. No additional licenses or subscriptions required for full functionality shall be excluded from the BOQ.
4. All required adapters, transceivers, optics, cabling, and connectivity components shall be included to meet the specified connectivity and performance requirements.

5. Support shall cover a minimum period of three (3) years.
6. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2.2.6.7.2 New Enterprise Storage

i. New Enterprise Storage - Primary Site

Item	Description	Qty
1.	All-NVMe Unified Storage Array	1
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2
3.	Controller Memory Cache (Minimum 384GB per controller, 768GB per array)	Included
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included
5.	NVMe TLC SSDs configured to deliver minimum 115TB usable capacity per array before data reduction	Lot
6.	Rack Mounting Kits and Accessories	Included
7.	Enterprise All-Inclusive Storage Software License Bundle covering all licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems	Lot
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of Primary Storage Systems.	Lot
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
10	Comprehensive instructor-led Storage Implementation, Administration, Operation, Security, Maintenance and Troubleshooting Training for Five (5) ICT Personnel at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	Lot
11	Any other component required for the successful implementation of the Enterprise digital solution	

ii. New Unified Enterprise All NVMe – DR Site

Item	Description	Qty
1.	All-NVMe Unified Storage Array	1
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2
3.	Controller Memory Cache (Minimum 256GB per controller, 512GB per array)	Included
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included
5.	NVMe TLC SSDs configured to deliver minimum **70TB usable capacity** per array before data reduction	Lot
6.	Rack Mounting Kits and Accessories	Included
7.	Enterprise All-Inclusive Storage Software License Bundle covering all licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems	Lot
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of DR Storage Systems.	Lot
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
10	Any other component required for the successful implementation of the Enterprise digital solution	

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. All SAN switches shall be supplied by the same manufacturer as the proposed storage solution.
4. All licenses required for operation, management, monitoring, diagnostics, analytics, trunking, and future port activation shall be included.
5. The solution shall support dual-fabric deployment across both Primary and Disaster Recovery sites.
6. Support subscriptions shall cover a minimum period of three (3) years.
7. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2.2.6.7.3 Storage Expansion For Existing Dell EMC Unity XT 480 Storage Arrays

Item No.	Description	Unit	Qty
1.	Dell EMC Unity XT 480 compatible expansion shelves including all required power supplies, fans, SAS cables, rail kits and installation accessories required for complete installation	Lot	
2.	SSD capacity expansion delivering a minimum of **20 TB usable capacity** configured in RAID 5 in Primary Site	Lot	
3.	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in Primary Site	Lot	
4.	NL-SAS capacity expansion delivering a minimum of **100 TB usable capacity** configured in RAID 6 in Primary Site	Lot	
5.	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot	
6.	NL-SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot	
7.	All licenses required to support the expanded capacity including snapshots, thin clones, replication, QoS, storage management, performance monitoring and data reduction features	Lot	
8.	Installation, configuration, testing, commissioning and integration services	Lot	
9.	Minimum Three (3) years OEM hardware and software support, including firmware updates and technical support	Lot	
10.	Any other item required to complete works/project		

Tenderers to disclose how they achieved the capacity in table below.

Site	Storage Tier	RAID Type	Required Usable Capacity	Proposed Drive Size	Proposed Number of Drives	Raw Capacity	Usable Capacity
Primary	SSD	RAID 5	20 TB				
	SAS	RAID 6	50 TB				
	NL-SAS	RAID 6	100 TB				
DR	SAS	RAID 6	50 TB				
	NL-SAS	RAID 6	50 TB				

Notes

1. The proposed solution is intended for the expansion of KPC's existing Dell EMC Unity XT 480 storage arrays and not for replacement of the existing systems.
2. All proposed hardware, software, drives, licenses, enclosures, cables, transceivers, drive carriers, mounting kits, and ancillary components required to achieve the specified capacities and maintain full OEM support shall be included in the tenderer's proposal even if not expressly listed in this BOQ.
3. All capacities quoted shall be usable capacities after RAID configuration and shall exclude system overheads unless otherwise stated.
4. The implementation shall be completed without disruption to production services and without requiring replacement of the existing storage arrays.

2.2.6.7.4 SAN Switches

i. SAN Switches for the Primary Site

Item	Description	Qty
1.	64-Port 64Gbps Enterprise SAN Switch	2
2.	64Gbps FC SFP56 Transceivers	64
3.	OM4 LC-LC Duplex Patch Cords (3m)	20
4.	Rack Mounting Kits and Accessories	Lot
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance and Troubleshooting Training for Five (5) System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot
9.	Any other component required for the successful implementation of the Enterprise digital solution	

ii. SAN Switches for the DR Site

Item	Description	Qty
1.	64-Port 64Gbps Enterprise SAN Switch	2
2.	64Gbps FC SFP56 Transceivers	64
3.	OM4 LC-LC Duplex Patch Cords (3m)	20
4.	Rack Mounting Kits and Accessories	Lot
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance and Troubleshooting Training for Five (5) System Administrators onsite.	Lot

Item	Description	Qty
9.	Any other component required for the successful implementation of the Enterprise digital solution	

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. Quantities of transceivers and patch cords are minimum requirements based on 32 active ports per switch.
4. All SAN switches shall be supplied by the same manufacturer as the proposed storage solution.
5. All licenses **required** for the operation of the proposed solution, including activated ports, fabric services, diagnostics, monitoring, management, and trunking, shall be included. The proposed switch shall support future port activation through software licensing without hardware replacement.
6. The solution shall support dual-fabric deployment across both Primary and Disaster Recovery sites.
7. Support shall cover a minimum period of three (3) years.
8. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2.2.6.7.5 Cloud Automation and Orchestration Platform

Item	Description	Qty
1.	Cloud Automation and Orchestration Platform for centralized management, orchestration, monitoring, automation, and lifecycle management of all proposed Servers, Storage systems, SAN infrastructure, network infrastructure, and related components.	Lot
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all proposed infrastructure assets into the platform.	Lot
3.	Administration, Operation and Maintenance Training for 5No. System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot
4.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Years
5.	All Licenses required to meet all the Cloud Automation and Orchestration Platform specifications	
6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)	

Notes

1. Pricing shall include all licenses, subscriptions, software components, connectors, agents, implementation services, training, documentation, and support necessary to meet all mandatory Cloud Automation and Orchestration Platform requirements.
2. No additional software, licenses, subscriptions, or modules shall be required to achieve full compliance with the Cloud Automation and Orchestration Platform requirements.

3. All prices shall include at least three (3) years of software subscription, updates, security patches, and 24x7 OEM support.

2.2.6.7.6 Database and High Availability Infrastructure

1. Database Engine & Platform Software Licensing			
Item	**Component Description**	**Sizing Metric / Unit**	**Declared Sizing Metric**
1.1	**Core Enterprise Database Software Licenses** *(Base engine licenses required to support primary and HA/DR workloads based on Tenderer's sizing)*	Per Core / Per CPU	
1.2	**In-Memory / Advanced Performance Options** *(In-memory, columnar, or partitioning add-ons required for full workload throughput)*	Per Core / Per RAM GB	
1.3	**High Availability & Replication Options** *(Engine-native replication, active-passive/active-active cluster options, or proxy software)*	Per Core / Per Node	
1.4	**Enterprise Security & Compliance Options** *(Transparent Data Encryption (TDE), data masking, auditing, and vault security)*	Per Core / Per Instance	
1.5	**Centralized Management & Monitoring Software** *(Enterprise management consoles, diagnostic/tuning packs, operational monitoring tools)*	Per Monitored Core	
1.6	**Database Proxy / Load Balancing Platform** *(Virtual IP management, connection pooling, read/write splitting, query routing appliances or software)*	Per Core / Per Node	
1.7	Three (3) Years OEM 24/7 Enterprise Software Support & Maintenance	Lot	
1.8	Training for five (5) on the proposed database clustering and High Availability Solution At the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	PAX	

1. Database Engine & Platform Software Licensing			
Item	**Component Description**	**Sizing Metric / Unit**	**Declared Sizing Metric**
	KPC will provide Air Tickets, accommodation and out off pocket allowance for the delegates		
1.9	Any other item required to meet all the specifications in the Database and High Availability Services Compliance Matrix (Attach a list with price for each line item)		

2. Database Infrastructure Sizing Declaration (Informational / Sizing Output for Infrastructure Team)- To fill by the tenderer				
This section carries $0 cost in this bid but forms a binding technical requirement for the separate Compute & Storage infrastructure provisioning.				
Item	**Component / Resource Type**	**Primary Site Sizing**	**DR Site Sizing**	**Total Sizing Declaration**
2.1	Total Allocated Compute (vCPU / Physical Cores)			
2.2	Total System Memory (RAM in GB) (Including dedicated in-memory allocation if applicable)			
2.3	Usable Storage Capacity (TB)			
2.4	Minimum Required Storage Performance*[Read/Write IOPS]*			[Peak Throughput MB/s]

Note:

1. Licensing Metrics: Tenderers must explicitly state their licensing model (e.g., Per Core, Per Processor, or Per User/Socket)
2. Engine-Specific Options: Tenderers proposing specialized appliances or engineered systems may bundle hardware and software line items, provided the hardware and OEM support components are clearly broken down.
3. Tenderers must guarantee that the total licensed cores listed above are sufficient to deliver the target performance, RPO, and RTO on the shared infrastructure.
4. Sizing Liability Clause: Tenderers are required to perform comprehensive workload sizing based on the transaction volumes, database sizes, and five years growth rate.
5. The software licenses priced in Section 1 must fully support the declared infrastructure requirements in Section 2. If, during implementation or commissioning, the proposed software core licenses prove insufficient to meet the performance SLAs, RPO, or RTO due to tenderer under sizing, the tenderer shall supply all additional required software licenses and OEM support at no additional cost to the Corporation.

2.2.6.7.7 Load Balancers/Application Delivery Controllers

Item	Description	Qty
1.	Application Delivery Controller (ADC) Appliances	4

Item	Description	Qty
2.	Centralized ADC Management Platform including Configuration Management, Analytics and Role-Based Administration	Lot
3.	ADC Configuration, Administration, Operations and Maintenance Training for 5No. Technical Team at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot
4.	Installation, Configuration and Integration with Datacenter Services	Lot
5.	All software licenses, subscriptions, and any other licenses required to fully meet all functional, operational, security, disaster recovery, high availability, and integration requirements specified in this tender document.	Lot
6.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot
7.	Any other item required to meet all the specifications in the Load Balancing Platform Compliance Matrix (Attach a list with price for each line item)	

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. No additional licenses or subscriptions required for full functionality shall be excluded from the BOQ.
4. Support subscriptions shall cover a minimum period of three (3) years.
5. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2.2.6.7.8 Enterprise System Monitoring and Response Platform

Item	Description	Qty
1.	Enterprise System Monitoring and Response Platform inclusive of all modules required to meet specifications in Enterprise System Monitoring and Response Platform Compliance Matrix	Lot
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all monitored objects	Lot
3.	Administration, Operation and Maintenance Training for 5No. Administrators at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot
4.	Minimum Three (3) Years 24x7x365 OEM Support, Updates Subscription, Security Patches and Firmware Updates	Years
5.	All Licenses required to meet all the specifications in Enterprise System Monitoring and Response Platform Compliance Matrix	
6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)	

2.2.6.7.9 Terminal Management System (TMS) BOM

The Tenderer shall provide a complete and fully itemized Bill of Materials for the Terminal Management System (TMS), Queue Management, Truck Inspection, Driver and Vehicle Management, Loading Operations and Loading Automation solution.

The BOM shall include all software, licences, terminal equipment, TMS-specific site infrastructure, interfaces, integration components, implementation services, training, warranty, support and other components required to provide a complete and operational solution across the approved KPC loading terminals.
The TMS shall support the five loading terminals identified in the tender baseline: **PS09, PS10, PS25, PS27 and PS28**

No.	TMS / Smart Loading Infrastructure Component	Licensing / Pricing Metric	KPC Baseline Quantity
1	**TMS Server and Compute Infrastructure**		
1.1	TMS Physical Enterprise Servers	Server	**10**
1.2	Server Operating System Licences	Server / Subscription	**10**
1.3	TMS Database Platform	Server / Core / Subscription	**5**
1.4	Database High Availability / Replication	Enterprise Licence	**5**
1.5	Rack-Mounted TFT Administration Monitor	Unit	**5**
2	**Queue Management Infrastructure**		
2.1	Outdoor Queue Display Screens (75-inch outdoor, IP65)	Display	**30**
3	**Driver and Vehicle Processing Infrastructure**		
3.1	RFID Readers (fixed, ultra-rugged; minimum quantity)	Unit	**30**
3.2	RFIDs Chips – reusable tags for trucks (see Reusable UHF RFID Tags specification)	Unit	**150,000**
3.3	RFID Printer / Encoder (see RFID Tag Printer specification)	Unit	**10**
4	**Inspection and Field Device Infrastructure**		
4.1	ATEX Inspection Tablets / Mobile Devices and accessories (ATEX-rated, for MSOOS)	Unit	**40**
5	**TMS Network and Communications Infrastructure**		
5.1	Fibre Optic Cabling	Metres	**2,100**

5.2	Structured Network Cabling	Lot	**48 Dual Data points per site (5 sites)**
5.3	Industrial Network Switches (PoE)	Unit	**5No- 48Ports**
5.4	Secure IP Communication Components	Lot	**2 No. Next-Generation DC Firewall Appliances (HA pair at primary DC – see Firewall specification)**
5.5	Network Transceivers, SFPs and Optics	Lot	**30No. - 1G 30No. - 10G**
5.6	Network Patch Cords and Accessories	Lot	**250No.-3m UTP Cables**
6	**Other Required Infrastructure Components**	Any other	

Notes

1. Quantities shall be validated through the approved site survey and detailed design for all applicable KPC locations.
2. The TMS scope covers five (5) terminals: PS09, PS10, PS25, PS27 and PS28. Integration is required with the Honeywell TMS at KPRL (PS15) and the COTAS system at PS12. The TMS covers truck loading at all five terminals, rail loading at Eldoret and Kisumu (configurable) and vessel loading at the jetties.
3. The Tenderer shall provide all hardware, software, licences, interfaces, connectivity, cabling, accessories and other components required for a complete operational solution.
4. Existing KPC equipment proposed for reuse shall be clearly identified, and the Tenderer shall confirm compatibility and any required upgrades or modifications.
5. All implementation, configuration, integration, testing, commissioning, training, documentation, warranty and support costs shall be included in the relevant BOM items.
6. Recurring costs, including licences, subscriptions, connectivity and OEM support, shall be separately identified.
7. TMS-specific site and edge infrastructure shall be included in this BOM. Common enterprise data-centre infrastructure shall be priced under the **Infrastructure BOM** to avoid duplication.
8. The Tenderer shall provide OEM make/model, part numbers, licence SKUs and licensing metrics for all proposed components.

2.2.6.8 *Implementation Services BOM*

2.2.6.8.1 Work breakdown structure detailed BOM

The tenderer shall fill this Work breakdown structure detailed BOM with relevant Deliverable outputs and Acceptance criterion

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
1	**Project initiation**				
1.1	Project mobilisation	Project Initiation Report	1	Lot	
1.2	Project management plan	PMP	1	Document	
1.3	Governance establishment	Governance Charter/RACI	1	Lot	
1.4	Integrated project schedule	Baseline Schedule	1	Lot	
1.5	RAID framework	RAID Register	1	Lot	
2	**Requirements & Business Process**				
2.1	Business process discovery	Process Catalogue		Process	
2.2	As-Is assessment & Process Re-engineering	As-Is Process Maps		Process	
2.3	To-Be design	To-Be Process Maps		Process	
2.4	Requirements validation	Requirements Catalogue		Requirement	
2.5	Fit-gap analysis	Fit-Gap Report		Module/Process	
2.6	Requirements baseline	Signed Requirements Baseline	1	Lot	
3	**Solution Architecture**				
3.1	Solution architecture	SAD	1	Lot	
3.2	Technical architecture	HLD/LLD	1	Lot	
3.3	Integration architecture	Integration Design	1	Lot	
3.4	Data architecture	Data Design	1	Lot	
3.5	Data Platform and Analytics Implementation				
3.6	Security architecture	Security Design	1	Lot	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
4	**Functional Configuration**				
4.1	ERP Modules configuration	Configured Module		Module	
4.2	MSOOS Configurations				
4.3	TMS Configurations				
4.4	Workflow configuration	Configured Workflow		Workflow	
4.5	Role configuration	Security Roles		Role	
4.6	All Reporting configurations	Standard Reports		Report	
5	**Customisation / Development**				
5.1	Simple development	Development Object		Object	
5.2	Medium development	Development Object		Object	
5.3	Complex development	Development Object		Object	
5.4	Custom reports	Report		Report	
6	**Integration**				
6.1	Applications interface	Interface		Interface	
6.2	IT/OT interface	Interface		Interface	
6.3	External interface	Interface		Interface	
6.4	API development	API		API	
7	**Data Migration**				
7.1	Data profiling	Data Quality Report		Data Object	
7.2	Data mapping	Mapping Specification		Object	
7.3	Data cleansing	Cleansed Dataset		Object	
7.4	Mock migration 1	Migration Report	1	Cycle	
7.5	Mock migration 2	Migration Report	1	Cycle	
7.6	Mock migration 3	Migration Report	1	Cycle	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
7.7	Production migration	Production Migration Report	1	Cycle	
8	**Infrastructure & Environments**				
8.1	Development environment	DEV	1	Environment	
8.2	Test environment	TEST	1	Environment	
8.3	UAT environment	UAT	1	Environment	
8.4	Production environment	PROD	1	Environment	
8.5	DR environment	DR	1	Environment	
9	**Cybersecurity & IAM**				
9.1	Role-Based Access Control (RBAC) Design & Implementation	Design and implement centralized RBAC	1	Report	
	Database & Application Security Controls	database and application controls	1	Report	
	ERP Application Security Configuration & Hardening	Harden ERP application servers, application components	1	Report	
	Security & Identity Integration Services	Integrate to SIEM,AD,PAM, SSO and MFA	1	Report	
	Professional Integration Service for One Identity Solution	Professional Integration Service	1		
	Security Documentation & Knowledge Transfer	Configuration documentation	Lot	Report	
	Security Administration Certification	comprehensive OEM-authorized	5No	Training	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
	Training for 5No staff at the Original Equipment Manufacturer's Approved Training Center. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	security training and certification			
10	**Testing & QA**				
10.1	Test strategy	Test Strategy	1	Document	
	UT	UT Report	1	Document	
10.2	SIT	SIT Report	1	Phase	
10.3	Regression testing	Regression Report	1	Phase	
	Security Testing	Security Test Report	1	Document	
10.4	Performance testing	Performance Report	1	Phase	
10.5	UAT	UAT Report	1	Phase	
10.6	Cutover rehearsal	Rehearsal Report		Cycle	
11	**Change Management**				
11.1	Change impact assessment	Impact Report	1	Lot	
11.2	Stakeholder engagement	Engagement Programme	1	Lot	
11.3	Business readiness	Readiness Report	1	Lot	
12	**Training & Knowledge Transfer**				
12.1	Training needs analysis	TNA	1	Lot	
12.2	End-user training	Training Sessions		Session	
12.3	Super-user training	Training Sessions		Session	
12.4	Technical training	Training Sessions		Session	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
12.5	Administrator training	Training Sessions		Session	
13	**Cutover & Deployment**				
13.1	Cutover strategy	Strategy	1	Document	
13.2	Cutover plan	Cutover Plan	1	Document	
13.3	Go-live	Production Deployment	1	Event	
13.4	Rollback capability	Rollback Plan	1	Plan	
14	**Hypercare**				
14.1	Hypercare support – 6 Months	Support		Month	
14.2	Incident resolution	Incident		Incident	
15	**Handover & Closure**				
15.1	Operational handover	Handover Pack	1	Lot	
15.2	As-built documentation	As-Built Pack	1	Lot	
15.3	Lessons learned	Lessons Learned	1	Document	
15.4	Final project closure	Closure Report	1	Lot	
15.5	24 Months SLA	SLA Agreement	1	Lot	

2.2.6.8.2 Tenderer Implementation services summary

WBS	Workstream	Fixed Price	Total Man-days
1	Project initiation & Mobilisation		
2	Requirements		
3	Architecture		
4	Configuration		
5	Development		
6	Integration		
7	Data and analytics platform		
8	Data Migration		
9	Infrastructure set-up		
10	Security		
11	Testing		
12	Change Management		
13	Training		
14	Cutover & Go-live		
15	Hypercare		
16	Support & Maintenance		
17	Handover/Closure		

2.2.6.8.3 Resources for key positions

The tenderer shall populate and provide a schedule of **named resources for key positions** with costings indicating the WBS the resources shall support

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days	Daily Rate	Total Cost	WBS Supported
R03	Project Manager	Day-to-day management	8+ yrs	Relevant						All
R04	Solution Architect	Overall architecture	10+ yrs	Relevant						
R05	Enterprise Architect	Architecture governance	10+ yrs	Relevant						
R06	Functional Lead ERP	Functional delivery	8+ yrs	Product						

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days	Daily Rate	Total Cost	WBS Supported
R06	Functional Lead MSOOS	Functional delivery	8+ yrs	Product						
R07	Functional Lead Data	Data migration	8+ yrs	Relevant						
R08	Technical Lead	Technical delivery	8+ yrs	Product/Technical						
R09	Integration Lead	Interfaces/ APIs	8+ yrs	Relevant						
R10	Testing Lead	Testing	8+ yrs	Relevant						
R11	Security Lead	Security/IAM	8+ yrs	Security						
R12	Test Manager	QA/test governance	8+ yrs	ISTQB or equivalent						
R13	Change Manager	Change/adoption	8+ yrs	Relevant						
R14	Training Lead	Training/KT	5+ yrs	Relevant						
R15	Senior Developer	Development	5+ yrs	Product						
R16	Functional Consultant	Configuration	5+ yrs	Product						
R17	Technical Consultant	Technical implementation	5+ yrs	Product						

Note:

i. **Governance and project management:** Establish a governance structure comprising the Steering Committee, PMO, business and technical workstreams, supported by a detailed integrated project plan, resource plan, risk management and regular progress reporting.

ii. **Tenderer responsibility:** Clearly identify assumptions, dependencies and KPC responsibilities, understand KPC's operational environment, and provide qualified resources throughout implementation.
iii. **Fit-gap analysis:** Conduct a comprehensive assessment covering standard functionality, configuration, customisation, integrations, process changes, regulatory and reporting requirements.
iv. **Solution architecture:** Develop comprehensive solution, application, data, integration, infrastructure, security and disaster recovery architectures capable of supporting future KPC growth.
v. **Integration and data migration:** Design, develop, test and document all required integrations and execute an approved data migration strategy.
vi. **Testing:** Perform comprehensive unit, system, integration, performance, security, migration, regression, user acceptance and disaster recovery testing, with documented evidence and defect management. No critical defects shall remain open at go-live.
vii. **Acceptance and payments:** All deliverables shall have predefined acceptance criteria and supporting evidence. Payments shall be linked to accepted milestone deliverables, and failed deliverables shall be corrected at no additional cost.
viii. **Training and knowledge transfer:** Provide role-based training, train-the-trainer programmes, knowledge transfer and competency evidence for business, technical and support teams.
ix. **Documentation:** Deliver complete requirements, design, architecture, configuration, customisation, integration, migration, security, testing, operational, training and as-built documentation.
x. **Go-live and support:** Conduct a formal Go-Live Readiness Review, obtain KPC approval, provide a six-month defect warranty and post-go-live hypercare, and formally transition operational responsibility to KPC.
xi. **Implementation costs:** Include travel, logistics, workshops, site visits, installation and commissioning costs unless explicitly excluded.
xii. **KPC responsibilities:** KPC will provide access to business users, available documentation, data extracts, workspace where applicable, connectivity, infrastructure access, subject-matter experts and timely approvals.

2.2.7 Additional Information to the Scope and Requirements

This forms part of the Terms of Reference and shall be read together with the preceding sections.

2.2.7.1 *General and interpretation*

- The Special Conditions of Contract (SCC) prevail over the General Conditions of Contract (GCC-IT) where they differ.
- Tenderers shall not scale down any baseline quantity stated in this tender. All BOM items are required; where a component is shared between BOM lines, the tenderer shall indicate the sharing. BOM lines apply equally to cloud and on premises offers; SaaS tenderers shall indicate the cost per BOM line.
- Licensing regimes and user groupings vary by solution. The current licence estate and the functional user groupings in this tender are provided for sizing; tenderers shall propose a licensing model that meets the stated requirements.
- Where this tender states that details will be provided at blueprinting, tenderers shall make reasonable, stated assumptions and price them within the fixed-price offer.
- Local content is not a preference criterion in this tender.

2.2.7.2 *Definitions*

- Banking Model: Refers to fungible products approach separating physical and book while reconciling the same at intervals.
- Partner countries are Uganda, South Sudan and Rwanda. Additionally, the destination countries include Democratic Republic of Congo (DRC), Burundi, Tanzania, Somalia, Sudan, Comoros Island, Mauritius, and Central African Countries.
- Partner terminals are terminals that are connected to the KPC pipeline network for receipt and/or transfer and hold stocks that are not part of KPC inventory. These include VTTI, GAPCO, PetroCity, Mombasa Joint, Nairobi Joint, Vivo, Rubis, OilCom e.t.c
- Marine receipt terminals are Kipevu Oil Storage Facility (KOSF) and KPRL
- The jetties are Kipevu Oil Terminal (KOT II), Shimanzi Oil Terminal (SOT) and Kisumu Oil Jetty (KOJ).
- CFA: Customer may import product as self-financed or financed by the Banks. Where it is financed by the banks through Collateral Finance Agreements (CFA), that product is held by KPC in trust and cannot be released to the customer without banks approval.
- ASE: ASE (Adjustment of Stock Entitlement) refers to the transfer of stocks entitlement from one customer to another.
- Pump-over operations occur at PS10, PS15 and PS14 and shall be configurable. Rail loading occurs at Eldoret and Kisumu (configurable); the hydrant system is COTAS; invoicing is performed in MSOOS.

2.2.7.3 *Solution scope boundaries*

- MSOOS is the single point of quantity conversion; the TMS returns gross and standardized volumes (GOV/GSV), density and temperature to MSOOS. The OMC portal is delivered with MSOOS. Operational demand forecasting for scheduling and ullage management is handled in MSOOS. Sales, demand and revenue forecasting is handled in the enterprise planning capability.
- Master data management shall be delivered within the proposed solutions and not as a separate product.
- All existing interfaces shall be rebuilt on the proposed integration platform. The tenderer shall provide all connectors, licences and other components necessary for the integrations, and shall disclose any third-party fees, proprietary formats or additional licences required by its solution.
- The Enterprise Document and Records Management System (EDRMS) is outside the scope of this tender. Integration with the EDRMS using CMIS and other open standards, including REST APIs, is in scope and shall be costed by the tenderer.
- Migration of relevant data from legacy systems is in scope; data up to the legally acceptable minimum period of seven (7) years shall be migrated with the detailed duration agreed at blueprinting.
- The minimum mock cycles provided is 3, however multiple mock migration cycles shall be required until open data errors and validation exceptions are less than 0.5% record reconciliation and 100% financial balances accuracy. KPC owns data quality decisions; the Contractor provides tools, profiling and cleansing support.

- Data-centre construction, network racks and cooling, replacement of the OT historian and SCADA, and pipeline optimisation are out of scope. KPC PLC will make available the OT integration interfaces; the tenderer shall ensure its solution integrates with the interfaces listed. The IT/OT DMZ and OT firewalls are out of scope; the design shall integrate with the existing ones following the IEC 62443 zone model (IT network – IT/DMZ firewall – industrial DMZ – OT firewall – OT network), with OT historians remaining in the OT zone.
- ANPR hardware is out of scope; ANPR integration via APIs and/or MQTT is in scope. ANPR is the primary and RFID the secondary vehicle-identification method.
- Where the TMS integrates directly with the Smith Meter AccuLoad controllers at PS09, PS10, PS25, PS27 and PS28, the TMS becomes the authorising host for preset, loading authorisation and transaction capture; the existing TAS (FuelFACS) is retained by KPC for historical and reporting purposes only; KPC will provide AccuLoad configuration data and TAS interface documentation during blueprinting.
- The TMS shall be deployed at the stations, with redundancy achieving RPO of 30 minutes and RTO of 2 hours.
- IT Service Management (ITSM) is part of the scope; the tenderer shall propose the ITSM solution.
- Existing identity and security platforms are OneIdentity (IAM), Arcon/Arcos (PAM) and FortiSIEM (SIEM); Any SIEM licence uplift is at KPC cost; log forwarding shall be via secure APIs. KPC has an existing F5 Web Application Firewall; the proposed solution shall integrate seamlessly with it.
- Embedded AI capability is required. The enterprise data analytics platform is preferably cloud-based, though alternatives are allowed; it is not subject to the in-country presence requirement but must comply with the Data Protection Act, 2019; anonymised analytics data may be held outside Kenya, and a no-copy approach is preferred.
- Data lineage to source is within scope and terminates at the interface where the source is outside scope.
- All custom components designs shall be approved by KPC PLC.
- Lot 2 executes organisational change management; Lot 1 (PMO) oversees it. Lot 1 provides continuous quality assurance for the 18-month implementation and the defect liability period, while the Independent QA partner (separate procurement) will provide quality assurance for all workstreams in both LOT 1 and LOT 2.

2.2.7.4 *Infrastructure, hosting and environments*

- MSOOS and TMS shall be deployed on KPC premises. Other components may be hosted on KPC premises or in an in-country cloud with verifiable evidence; cloud terms must meet the Data Protection Act and Critical Information Infrastructure regulations.
- Cloud services provider SLAs are accepted where they meet the requirements of this tender; data residency applies to production and non-production environments; tenderers shall submit the OEM cloud master agreements.
- Testing of High Availability shall require witnessed failover of non-production environment.

- Environments: DEV, TEST/QA, UAT and PROD on both the primary and DR sites, with resources skewed towards the primary site. The QA environment serves all testing, including UAT. An evergreen environment is included in the baseline. Primary and DR shall be at different physical sites. RTO of 2 hours and RPO of 30 minutes apply to the all platforms including integration and every interface; a full failover DR test is required, and pre-go-live DR tests shall be as many as necessary.
- The 688 primary and 412 DR cores are for the new workload; Intel or AMD x86 servers are acceptable. Servers shall support the specified GPU capability, but GPUs are not part of the build in this project. Tenderers shall provide Enterprise Linux OR Windows Server licensing sufficient for the full compute capacity, including VM and container workloads, HA, workload mobility, failover, DR and maintenance, without additional licensing. Existing VMware licences shall be ignored; VMware/virtualisation licences shall be provided as per the specifications and BOM. Equivalent NIC models with equal or better port count, speed and features, and equivalent RAID controllers (RAID 0, 1, 5, 6, 10, 50, 60), are acceptable.
- Storage: NVMe TLC SSDs are required for the primary and DR arrays; the primary array is one lot delivering at least 115 TB usable before data reduction. Storage controllers using other enterprise-grade processor architectures are acceptable if they meet or exceed the stated performance. A SAN trunking licence is not required; tenderers shall include spare disks. Existing backup infrastructure comprises LTO-8/9 tape and a Veritas/Cohesity Access appliance.
- Analytics storage: the 5 TB baseline is provisioned storage capacity; the 11% annual growth applies to the overall footprint; sizing shall cover all data-lifecycle layers (raw, cleansed, transformed, curated, analytical, indexes, temporary space, replicas and backups) and shall be based on raw, uncompressed volumes – deduplication/compression may be shown only as a separate line item. Log retention: hot 90 days, cold 12 months (online searchable 12 months), frozen up to 36 months, with policy-based movement between tiers without data loss.
- Network switches: MACsec shall be supported on access and uplink ports; fabric, advanced Layer 3 and stacking functions shall be available without recurring licences (any required licences shall be perpetual and included in the bid price). Application delivery controllers: models exceeding the specified performance are acceptable provided all interface and connectivity requirements are met or exceeded; two ADC appliances shall be provided per site (active-active at primary, active-standby at secondary) with automatic failover and all HA licences.
- Integration/API: API measures are in transactions per second, with 11% annual growth; message sizes are variable.
- Penetration testing by authorised providers is required before go-live and shall be responsibility of an independent QA contractor.
- Performance testing shall be at peak volumes on production-equivalent infrastructure; the tenderer provides the testing tools.

2.2.7.5 *Commercial and contractual*

- Implementation is eighteen (18) months from kick-off, ending at Go-Live; alternative release strategies are encouraged. Hypercare is 6 months per release. Warranty is three (3) years for all equipment, with on-site support. Implementation support is two (2) years; hardware support and OEM software maintenance three (3) years.
- Software licenses prices are fixed for six (6) years, and growth is charged at the fixed unit prices.
- A parent-company letter of undertaking suffices for the parent company guarantee. The performance security covers the period up to the 90 days after the Final Acceptance Certificate.

2.2.7.6 *User baselines (for sizing)*

- Approximately 1,500 employees (headcount); Employee Self-Service 1,500 users; Manager Self-Service 150 users; 500 named HR users; GRC: 70 approvers and 27 administrators of roles and rule sets; safety management 90 users; contract lifecycle management 100 users; CRM 30 internal and 70 external users; budgeting, planning and consolidation approximately 70 users.

PART 2 – TENDER FORMS

SECTION III: TENDER SUBMISSION FORMS

Tenderers shall complete all applicable forms and submit them through the SAP SRM portal. Technical Proposal forms (TP-IT-1 through TP-IT-8) and Financial Proposal forms (FP-IT-1 through FP-IT-2) are submitted in separate workspaces on the portal. Forms may be reproduced on the Tenderer's letterhead provided all content is retained.

FORM TP-IT-1A: TECHNICAL PROPOSAL SUBMISSION FORM

Date: _____ Tender Ref: _____

To: General Manager — Supply Chain, Kenya Pipeline Company PLC

We, the undersigned, submit our Technical Proposal for [Project Title] and confirm:

1. We have read and understood the full Tender Documents;
2. We have no conflict of interest (or have disclosed conflicts in Form COI-IT);
3. We are eligible and not debarred by KPC PLC or subject to insolvency proceedings;
4. Our Technical Proposal contains NO financial or cost information;
5. The proposed solution meets or exceeds the Technical Specifications/Terms of Reference (deviations listed in TP-IT-4);
6. We commit to provide a Proof of Concept or scripted demonstration if required, at our own cost;
7. All OEM authorisations are current and attached as Form OEM-IT;
8. We comply with KPC PLC's cybersecurity requirements (Form CS-IT attached);
9. We comply with the Data Protection Act 2019 (Form DPD-IT attached);
10. We will sign the Contract and provide Performance Security within 10 working days of award.

Firm Name: _____

Authorised Signature: _____

Name and Title: _____

Date: _____

FORM TP-IT-1B - CONSORTIUM AGREEMENT – to be submitted for LOT 2 – Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution.

(Complete where Tenderer is a Consortium. **Fully Executed Consortium Agreement to be attached**.)

This Agreement is entered into on _____ by and among:
[Name of Lead Member] — hereinafter 'Lead Member'
[Name of Member 2]
[Name of Member 3] (etc.)

The parties hereby agree as follows:

1. All members shall be jointly and severally liable for the full performance of the Contract.
2. [Name of Lead Member] is hereby authorised to act as Lead Member and to bind the Consortium in all matters related to this tender and any resulting Contract. The Lead Member has authority to bind all members; the composition approved tender shall not change without the KPC PLC's prior written approval; and each member's scope shall be disclosed in the Consortium Schedule.
3. The respective roles, responsibilities and shares of each member are as follows: [describe]
4. The composition of the Consortium shall not be altered without the prior written consent of KPC PLC.
5. The consortium agreement shall be accompanied by a notarized power of attorney.
6. This Agreement shall be governed by the laws of Kenya.

Lead Member Signature: _____ Name: _____ Date: _____

Member 2 Signature: _____ Name: _____ Date: _____

FORM TP-IT-2A: TENDERER PROFILE AND CORPORATE CREDENTIALS

All tenderers including all members of a Consortium must fill this form

Full Registered Name	
Type of Entity	Company / Partnership / Consortium/ Other
Country of Incorporation	
Year Established	
Company Registration / Certificate of Incorporation	
VAT Registration No. for Local Companies/ Tax Registration for Foreign Companies	
Primary Business	IT Solutions / System Integration / OEM / VAR / MSP / Other
Physical Address	
Email	
Telephone	
Website	
Contact Person for this Tender	
Contact Email / Phone	
Total Staff (Kenya)	IT Technical: ___ / Support: ___ / Other: ___
Annual Revenue (last 3 years — USD) Attach Audited Financial Statements Supporting the Figures Stated.	Year 1: ___ / Year 2: ___ / Year 3: ___
IT Certifications Held	[e.g., ISO/IEC 27001, ISO 9001, CMMI, SOC 2]
OEM Partnership Status for Solutions Under Bid (ERP, MSOOS, Middleware, Analytics, e-Procurement, e-HR, Hardware and Platform)	
Is this a Consortium?	Yes / No — if Yes, list all members and roles

FORM TP-IT-2B: TENDERERS RELEVANT EXPERIENCE

LOT 1: Comparable Assignments (Last 7 years — provide minimum 3 projects)

The Respondent shall provide details of projects undertaken within the period specified in the Tender that demonstrate experience relevant to the lot being applied for. Additional project sheets may be attached where necessary.

Project Reference No. _____

Item	Details
Project Title	
Client / Organization	
Country	
Industry / Sector	
Contract Value (USD/KES)	
Contract Duration	From: _____ To: _____
Completion Status	☐ Completed ☐ Ongoing
Tenderer's Role	☐ Prime Contractor ☐ Consortium Lead ☐ Consortium Member ☐ Subcontractor
Percentage of Tenderer's Participation	_____%
Client Contact Person	
Designation	
Telephone	
Email	

Scope of Services Delivered

Provide a brief description of the scope of work performed, including the **products, product versions**, **services**, and **responsibilities** undertaken by the Respondent.

Relevance to this Tender

Tick all that apply.

Relevant Experience Area	Applicable
Programme / Programme Management Office (PMO)	☐
Enterprise Resource Planning (ERP)	☐
MSOOS & TMS	☐
Enterprise Integration Platform / Middleware	☐

Relevant Experience Area	Applicable
Infrastructure	☐
Cybersecurity	☐
Change Management & Training	☐
Data Migration	☐
Other (Specify)	

Client Reference

Requirement	Response
Completion Certificate attached	☐ Yes ☐ No
Client Reference Letter attached	☐ Yes ☐ No
Contract / Purchase Order attached (where available)	☐ Yes ☐ No
Evidence Reference (Document / Page No.)	

Declaration

I/We certify that:

1. The information provided in this form is true and accurate.
2. The projects listed were undertaken by the Respondent or, where applicable, by the consortium member identified in the submission.
3. KPC PLC may contact the listed clients to verify the information provided.
4. Supporting documentary evidence has been attached for each project.

Authorised Signatory: _____

Name & Position: _____

Signature: _____

Date: _____

Company Stamp/Seal: _____

LOT 2: Last 10 Years provide minimum 3 Projects

The Respondent shall provide details of projects undertaken within the period specified in the Tender that demonstrate experience relevant to the lot being applied for. Additional project sheets may be attached where necessary.

Project Reference No. _____

Item	Details
Project Title	
Client / Organization	

Country	
Industry / Sector	
Contract Value (USD/KES)	
Contract Duration	From: _____ To: _____
Completion Status	☐ Completed ☐ Ongoing
Tenderer's Role	☐ Prime Contractor ☐ Consortium Lead ☐ Consortium Member ☐ Subcontractor
Percentage of Tenderer's Participation	_____%
Client Contact Person	
Designation	
Telephone	
Email	

Scope of Services Delivered

Provide a brief description of the scope of work performed, including the **products**, **products' versions, services**, and **responsibilities** undertaken by the Respondent. Highlight any benefits accrued by the customer

Relevance to this Tender

Tick all that apply.

Relevant Experience Area	Applicable
Programme / Programme Management Office (PMO)	☐
Enterprise Resource Planning (ERP)	☐
MSOOS & TMS	☐
Enterprise Integration Platform / Middleware	☐
Infrastructure	☐
Cybersecurity	☐
Change Management & Training	☐
Data Migration	☐
Other (Specify)	

Client Reference

Requirement	Response
Completion Certificate attached	☐ Yes ☐ No

Client Reference Letter attached	☐ Yes ☐ No
Contract / Purchase Order attached (where available)	☐ Yes ☐ No
Evidence Reference (Document / Page No.)	

Declaration

I/We certify that:

5. The information provided in this form is true and accurate.
6. The projects listed were undertaken by the Respondent or, where applicable, by the consortium member identified in the submission.
7. KPC PLC may contact the listed clients to verify the information provided.
8. Supporting documentary evidence has been attached for each project.

Authorised Signatory: _____

Name & Position: _____

Signature: _____

Date: _____

Company Stamp/Seal: _____

FORM TP-IT-3: TECHNICAL SOLUTION DESCRIPTION – For LOT 2 Only

Describe the proposed solution comprehensively covering all systems and subsystem, infrastructure and security elements in scope. This is the core of the Technical Proposal.

Include:

i. Provide an overview of the Offer covering all aspects of the tender for design, supply, implementation, commissioning, support and maintenance of an enterprise digital solution.
ii. Complete Solution Architecture Diagram — showing all hardware, software, network and integration layers
iii. Hardware: Make, model, specification, country of manufacture, warranty terms
iv. Software/Applications: Vendor, product name, version, licensing model (perpetual/subscription/SaaS)
v. Licences: Type, number of users/nodes/CPUs, duration, renewal conditions
vi. Integration: How the proposed solution integrates with KPC PLC's existing systems listed in requirements. Provide an inventory of all the connectors to be used in the integration
vii. Cloud/On-Premise/Hybrid architecture and rationale
viii. Scalability — how the solution grows with KPC PLC's needs over 5 years
ix. Redundancy, High Availability and Disaster Recovery capabilities
x. Data residency — where data will be stored and processed

xi. Security architecture — identity management, access controls, audit logs, monitoring and risk management within the system

xii. Detail out how the solution in the proposed architecture meets each requirement in the Technical and Functional Specifications

xiii. Product Road Map for the next 10 Years

xiv. Attach product data sheets for all software and hardware

xv. Attach standard licence master agreement for all software and cloud service agreement from the OEM.

xvi. Attach certifications and recognitions for the product/solution from the OEM where applicable especially for Infrastructure, MSOOS and ERP

FORM TP-IT-4: TECHNICAL COMPLIANCE MATRIX – LOT 2 Only

Complete for every requirement in the Functional and Technical Specifications/Terms of Reference. State where the feature is available as Standard or Customized Development or Not Available.

Ref.	Functional and Technical Requirement	Proposed Solution	Compliance Status (Standard/Customized Development/Not Available)	Evidence (Page No. of Data Sheet)
1	[From Technical Specifications/Terms of Reference]			
2	[From Technical Specifications/Terms of Reference]			
3	[From Technical Specifications/Terms of Reference]			
4	[From Technical Specifications/Terms of Reference]			
5	[From Technical Specifications/Terms of Reference]			
6	[From Technical Specifications/Terms of Reference]			

FORM TP-IT-5A: PROJECT MANAGEMENT METHODOLOGY – LOT 1

Provide a detailed Implementation Plan for each Lot covering:

i. Project Management Methodology complete with governance structure, risk management, change management, knowledge management and resource management
ii. Project Phases with milestones addressing and achieving all the requirements in the terms of reference.
iii. Resource Plan: Project team structure, roles and responsibilities (Tenderer's and KPC PLC's counterpart team)
iv. Gantt Chart showing all activities, dependencies, milestones and deliverables with timelines
v. Change Management and Training Plan: user training approach, training materials, train-the-trainer programme
vi. Cut-off Plan complete with Go-Live prerequisites, Go-Live activities, Hypercare and Stabilisation Period: post-Go-Live support intensity and duration
vii. Project management and Reporting Templates

FORM TP-IT-5B: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN – LOT 2

Provide a detailed Implementation Plan for each Lot covering:

i. Detailed Implementation Approach including methodology
ii. Project Phases with milestones: Milestone Gates and Checklist
iii. Resource Plan: Project team structure, roles and responsibilities (Tenderer's and KPC PLC's counterpart team)
iv. Gantt Chart showing all activities, dependencies, milestones and deliverables with timelines
v. Data Migration Strategy
vi. Change Management Strategy
vii. Testing Strategy
viii. Go-Live and Cut Over Strategy
ix. Hypercare and Stabilisation Period: post-Go-Live support intensity and duration
x. Knowledge Transfer
xi. Tools to accelerate design, deployment, Data migration, Testing and end user Training
xii. Training Strategy
xiii. Provide schedule of available Technical, functional, User and Executive courses for key solutions and must include ERP, MSOOS, Analytics, e-Procurement, e-HR, Hardware, OS, Database, High Availability, Platform, Development

FORM TP-IT-6: PROPOSED TEAM — KEY PERSONNEL

Provide the project team structure and completed CVs for all Key Personnel.

No.	**Proposed Position**	**Name of Proposed Expert**	**Employer** ***(Tenderer / Consortium Member / Subcontractor)***	**Years of Relevant Experience**	**Highest Qualification**	**Professional Certifications**	**Relevant Project Experience** ***(No. of Similar Projects)***	**CV Reference**
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

For each Key Personnel, provide a CV (maximum 3 pages per person) including:

i. Full name; current role with the Tenderer
ii. Academic qualifications (degree, institution, year)
iii. Professional certifications
iv. If English is not First Language state the Level of Proficiency
v. Total years of IT experience; **years with current firm**
vi. Relevant project experience (last 7 years) — project name, client, role, technologies, outcome
vii. Statement of availability for this project
viii. Duly Signed by the personnel and the Tenderer

FORM TP-IT-7: AFTER-SALES SUPPORT AND SERVICE LEVEL AGREEMENT PROPOSAL

Describe the proposed Support and Maintenance regime, including:

- Support model: on-site / remote / hybrid; escalation matrix
- Help Desk: contact channels, operating hours, response time by ticket severity
- Proposed SLA Parameters (state what is offered for each):

No.	SLA Parameter	KPC PLC Minimum Requirement	Tenderer's Proposed Level
1	System Uptime	99.7% excluding planned maintenance	
2	Critical (P1) Incident Response	Acknowledge: 15 min; Resolution: 2 hours	
3	High (P2) Incident Response	Acknowledge: 30 min; Resolution: 8 hours	
4	Medium (P3) Incident Response	Acknowledge: 2 hours; Resolution: 24 hours	
5	Low (P4) Service Request	Acknowledge: 4 hours; Resolution: 5 business days	
6	Planned Maintenance Window	Agreed in advance; off-peak hours only	
7	Patch/Security Update Deployment	Critical: 48 hours; Others: 30 days	
8	Backup Frequency and RTO/RPO	Daily backup; RTO: 2 hours; RPO: 30 Minutes	
9	Disaster Recovery	BCP/DR test Quarterly	

i. Service Credits / Penalties: proposed service credit mechanism for SLA breaches
ii. Spare Parts Management (for hardware): local spare parts inventory; source and lead times for critical components
iii. Software Updates and Version Upgrades: what is included in the AMC; what is charged additionally
iv. Security Incident Response: breach notification procedure; forensic support capability
v. Offshore Support: where offshore support is used, specify location, data access controls, privacy measures
vi. Tenderers should attach their standard SLAs terms where applicable.

FORM TP-IT-8A PART 1: CYBERSECURITY AND DATA PROTECTION DECLARATION

SECTION A — CYBERSECURITY COMPLIANCE OF THE FIRM – LOT 1 AND LOT 2

No.	Cybersecurity Requirement	Evidence / Certification	Compliant?
1	ISO/IEC 27001 Certification or equivalent	Certificate / Audit Report	
2	Compliance with Kenya Data Protection Act 2019	DPA compliance statement	

SECTION B — DATA PROTECTION COMPLIANCE

1. All personal data provided by KPC PLC will be processed only for purposes of this project;
2. Technical and organisational security measures are in place to protect KPC PLC's data;
3. Data will not be transferred outside Kenya without KPC PLC's prior written approval;
4. Any personal data breach will be notified to KPC PLC within 24 hours of discovery;
5. All KPC PLC data will be returned or securely destroyed at project completion;
6. The Tenderer will execute a Data Processing Agreement (DPA) before project commencement.

Authorised Signature: _____

Date: _____

FORM TP-IT-8 PART 2: CYBERSECURITY AND DATA PROTECTION DECLARATION

SECTION A — CYBERSECURITY COMPLIANCE OF THE SOLUTIONS – LOT 2 ONLY

No.	Cybersecurity Requirement	Evidence / Certification	Compliant?
1	ISO/IEC 27001 Certification or equivalent	Certificate / Audit Report	
2	SOC 2 Type II Report (for cloud/managed services)	Report from accredited auditor	
3	Data Encryption: at rest and in transit	Technology description	
4	Access Control: Role-Based Access Control (RBAC) implemented	Architecture description	
5	Multi-Factor Authentication (MFA) for administrative access	System capability description	

6	Vulnerability Management Programme in place	Policy and tooling description	
7	Security Information and Event Management (SIEM)	Integration capability description	
8	Incident Response Plan: documented and tested	OEM IRP document reference	
9	Compliance with Kenya Data Protection Act 2019	DPA compliance statement for the proposed solutions	

SECTION B — DATA PROTECTION COMPLIANCE

1. All personal data provided by KPC PLC will be processed only for purposes of this project;
2. Technical and organisational security measures are in place to protect KPC PLC's data;
3. Data will not be transferred outside Kenya without KPC PLC's prior written approval;
4. Any personal data breach will be notified to KPC PLC within 24 hours of discovery;
5. All KPC PLC data will be returned or securely destroyed at project completion;
6. The Tenderer will execute a Data Processing Agreement (DPA) before project commencement.

Authorised Signature: _____

Date: _____

FORM TP-IT-9: TECHNICAL BILL OF MATERIAL

LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES

Provide a non-costed bill of materials with all the components required to successfully manage and deploy this project. All the items must be well described with PMO Service, Description, Unit, Qty. This bill of material should be aligned to the financial proposal which is submitted separately.

LOT 2: DESIGN, SUPPLY, IMPLEMENATION, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL TRANSFORMATION SOLUTION

Provide a non-costed bill of materials with all the components required to successfully **Design, Supply, Implement, Support and Maintain the proposed Enterprise Digital Solution**. All the items must be well described inclusive of part numbers, metrics, quantities and grouped as per the architecture for ease of understanding. This bill of material should be aligned to the financial proposal which is submitted separately. **The BoM must include all components required to Design, Supply, Implement, Support and Maintain the proposed Enterprise Digital Solution.**

In addition to the complete and non-priced BoM mentioned in the paragraph above the tenderer should fill and submit the following tables. Where the grouping of the licences are not as outlined in the tables the tenderer is free to indicate how the licence requirement has been met including stating their own licencing metric.

9A Business Applications BOM

No.	Business Application / Capability	Licensing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
1	Financial Operations	Users	300			
2	Supply Chain Management	Users	900			
3	Human Capital Management	Users	1,500			
4	Payroll	Payroll Load	1,500			
5	Enterprise Asset Management	Users	600			
6	Project Lifecycle Management	Users	200			
7	Strategic Planning and Performance Management	Users	100			
8	Enterprise Risk Management	Users	100			
9	Identity, access control, Multi-Factor and SSO	Users	1500			
10	Customer Relationship Management (CRM)	Users	50			
11	E- Procurement	Users	500			
12	Contract Lifecycle Management (CLM)	Users	100			
13	Sales and Commercial Management	Users	50			
14	Safety Management	Users	1500			
15	IT Service Management (ITSM)	Users	50			
16	Enterprise Monitoring and Observability	Users	30			
17	Integrated Development	Users(developers)	20			

No.	Business Application / Capability	Licensing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
	platform and workflow & Business Process Automation					
18	Integration platform	Integration Points	All Integration points			
19	Comprehensive instructor-led certification training for 60No staff Functional Superuser ERP training Solution at OEM's authorized training center that has been in operation for atleast 5 years	Pax	60No			
20	Include any other component necessary for the solution to meet all the functional and technical requirements.	LOT	LOT			
21	Annual Maintenance and support if applicable	LOT				

9B Mid-Stream Oil Operations Solution and Terminal Management Solution BOM

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
1	**Order & Inventory Management**	Order management, inventory management, quantity conversion and standardisation	User / Enterprise	1 LOT			
2	**Nominations, Scheduling & Demand Forecasting**	Nominations, scheduling, allocation, capacity planning and demand forecasting	User / Enterprise	1 LOT			
3	**Terminal Management**	Terminal operations, truck/driver management, loading operations, loading station/arm management, gate and queue management	Terminal / Loading Station	1 LOT			
4	**Quality Control Management**	Product quality management, inspection, quality records and certificates	User / Enterprise	1 LOT			
5	**MSOOS Certification Training**	Comprehensive instructor-led certification training on 20No MSOOS Solution at OEM's	Pax	20No			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
		authorized training center that has been in operation for atleast 5 years					
6	**Other Required Components**	Any additional licences, modules, interfaces, middleware, software or services required for a complete solution	LOT	1			

9C Enterprise Data Analytics BOM

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
1	**Enterprise Data & Analytics Platform**	Cloud data lake/Lakehouse, analytical platform, storage and processing capacity for 5 TB initial data with 10% annual growth	Subscription / Consumption	**1 LOT**			
2	**Data Integration**	ETL/ELT, API, CDC, batch and	Subscription /	**1 LOT**			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
	& Data Engineering Platform	near-real-time integration, orchestration and data quality	Consumption				
3	**Enterprise AI, Machine Learning, Data Science & Generative AI Platform**	AI/ML, data science, model development and MLOps, predictive and prescriptive analytics, forecasting, anomaly detection, Generative AI, natural-language analytics, intelligent recommendations and AI-assisted decision support	Subscription / Consumption	**1 LOT**			
4	**Data Governance, Security & Metadata Management**	Data catalogue, metadata, lineage, data quality, access control, audit, privacy and AI/ML governance	Subscription / Consumption	**1 LOT**			
5	**Power BI Integration**	Integration with KPC's existing Power BI environment, semantic models, analytical datasets, AI outputs and governed reporting data	Integration / LOT	**1**			
6	**Enterprise Systems & External Data Integration**	Integration with ERP/Core System, TMS, EAM, HR, ITSM, operational systems, IoT/SCADA and approved external data sources	Integration / LOT	**1**			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
7	**Cloud Infrastructure, HA, Backup & DR Services**	Compute, storage, network/data transfer, high availability, backup, disaster recovery, monitoring and security services	Subscription / Consumption	**1 LOT**			
8	**Implementation, Deployment & Priority AI/Analytics Use Cases**	Requirements validation, detailed solution architecture, platform configuration, data integration, testing, commissioning, and development/deployment of 5 agreed priority AI and advanced analytics use cases	LOT	**1**			
9	**Analytics/ML Certification Training**	Comprehensive instructor-led certification training on 12No AI/ML and analytics training Development at OEM's authorized training center that has been in operation for atleast 5 years	Pax	12No			
10	**Knowledge Transfer**	Administration, data engineering, data science, AI/ML and analytics training	Pax	**30No**			
11	**Support, Maintenance, Updates &**	24×7 support, platform maintenance,	Annual Subscription	**5 Years**			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Proposed OEM / Product	Proposed Tenderer Licence Quantity	Tenderer Comments on metric or licences clustering
	Technical Assistance	software updates, security patches, upgrades and technical assistance					
12	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**			

9D Enterprise Middleware & Application Development Platform BOM

No.	BOM Component	Description / Scope	License Metric	Estimated Qty.	Tenderer Proposed Quantity
1	**Integration Platform**	Core middleware / integration platform	Lot	1	
2	**API Management Platform**	API publishing, lifecycle management and governance	Lot	1	
3	**Enterprise Service Bus (ESB)**	Service orchestration and application integration	Lot	1	
4	**Message Broker**	Asynchronous messaging and event distribution	Lot	1	
5	**Event Streaming Platform**	Real-time event streaming and processing	Lot	1	
6	**Workflow / Orchestration Engine**	Process orchestration across systems	Lot	1	
7	**Data Transformation Engine**	Mapping, transformation and enrichment	Lot	1	
8	**Integrations and Application Development Certification**	Comprehensive instructor-led certification training on 15No Integrations and Application Development at OEM's authorized training	Pax	15No	

		center that has been in operation for atleast 5 years			
9	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**	

9E Infrastructure BOM

9E.1 Compute Platform

i. Compute Platform – Primary Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	Enterprise x86 Rack Servers	6			
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot			
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot			
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot			
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
6.	Comprehensive instructor-led certification training on operating system and security administration, virtualization, containerization, database and performance tuning Training for Proposed Compute Platform for 5No. System Administrators at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	5			
7.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.				

ii. Compute Platform – DR Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	Enterprise x86 Rack Servers	4			
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot			
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot			
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot			
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
6.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.				

9E.2 New Enterprise Storage

i. New Enterprise Storage - Primary Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	All-NVMe Unified Storage Array	1			
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2			
3.	Controller Memory Cache (Minimum 384GB per controller, 768GB per array)	Included			
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included			
5.	NVMe TLC SSDs configured to deliver minimum 115TB usable capacity per array before data reduction	1 Lot			
6.	Rack Mounting Kits and Accessories	Included			
7.	Enterprise All-Inclusive Storage Software License Bundle covering all	Lot			

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
	licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems				
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of Primary Storage Systems.	Lot			
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
10	Comprehensive instructor-led Storage Implementation, Administration, Operation, Security, Maintenance and Troubleshooting Training for Five (5) ICT Personnel at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	Lot			
11	Any other component required for the successful implementation of the Enterprise digital solution				
	Subtotal				
	Applicable Taxes				
	Grand Total				

ii. New Unified Enterprise All NVMe – DR Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	All-NVMe Unified Storage Array	1			

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2			
3.	Controller Memory Cache (Minimum 256GB per controller, 512GB per array)	Included			
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included			
5.	NVMe TLC SSDs configured to deliver minimum **70TB usable capacity** per array before data reduction	Lot			
6.	Rack Mounting Kits and Accessories	Included			
7.	Enterprise All-Inclusive Storage Software License Bundle covering all licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems	Lot			
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of DR Storage Systems.	Lot			
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
10	Any other component required for the successful implementation of the Enterprise digital solution				

9E.3 Storage Expansion For Existing Dell EMC Unity XT 480 Storage Arrays

Item No.	Description	Unit	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
	Dell EMC Unity XT 480 compatible expansion shelves including all required power supplies, fans, SAS	Lot				

Item No.	Description	Unit	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
	cables, rail kits and installation accessories required for complete installation					
	SSD capacity expansion delivering a minimum of **20 TB usable capacity** configured in RAID 5 in Primary Site	Lot				
	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in Primary Site	Lot				
	NL-SAS capacity expansion delivering a minimum of **100 TB usable capacity** configured in RAID 6 in Primary Site	Lot				
1.	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot				
2.	NL-SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot				
	All licenses required to support the expanded capacity including snapshots, thin clones, replication, QoS, storage management, performance monitoring and data reduction features	Lot				
	Installation, configuration, testing, commissioning and integration services	Lot				
	Minimum Three (3) years OEM hardware and software support, including firmware updates and technical support	Lot				
3.	Any other item required to complete works/project					

Tenderers to disclose how they achieved the capacity in table below.

Site	Storage Tier	RAID Type	Required Usable Capacity	Proposed Drive Size	Proposed Number of Drives	Raw Capacity	Usable Capacity
Primary	SSD	RAID 5	20 TB				
	SAS	RAID 6	50 TB				
	NL-SAS	RAID 6	100 TB				
DR	SAS	RAID 6	50 TB				

	NL-SAS	RAID 6	50 TB				

9E.4 SAN Switches

i. SAN Switches - Primary Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	64-Port 64Gbps Enterprise SAN Switch	2			
2.	64Gbps FC SFP56 Transceivers	64			
3.	OM4 LC-LC Duplex Patch Cords (3m)	20			
4.	Rack Mounting Kits and Accessories	Lot			
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot			
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot			
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance and Troubleshooting Training for Five (5) System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot			
9.	Any other component required for the successful implementation of the Enterprise digital solution				

ii. SAN Switches – DR Site

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	64-Port 64Gbps Enterprise SAN Switch	2			
2.	64Gbps FC SFP56 Transceivers	64			
3.	OM4 LC-LC Duplex Patch Cords (3m)	20			

4.	Rack Mounting Kits and Accessories	Lot			
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot			
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot			
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance and Troubleshooting Training for Five (5) System Administrators onsite.	Lot			
9.	Any other component required for the successful implementation of the Enterprise digital solution	Lot			

9E.5 Cloud Automation and Orchestration Platform

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	Cloud Automation and Orchestration Platform for centralized management, orchestration, monitoring, automation, and lifecycle management of all proposed Servers, Storage systems, SAN infrastructure, network infrastructure, and related components.	Lot			
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all proposed infrastructure assets into the platform.	Lot			
3.	Administration, Operation and Maintenance Training for 5No. System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot			
4.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Years			
5.	All Licenses required to meet all the Cloud Automation and Orchestration Platform specifications	Lot			

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)	Lot			

9E.6 Database and High Availability Infrastructure

3. Database Engine & Platform Software Licensing

Item	Component Description	Sizing Metric / Unit	Declared Sizing Metric	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.1	**Core Enterprise Database Software Licenses** *(Base engine licenses required to support primary and HA/DR workloads based on Tenderer's sizing)*	Per Core / Per CPU				
1.2	**In-Memory / Advanced Performance Options** *(In-memory, columnar, or partitioning add-ons required for full workload throughput)*	Per Core / Per RAM GB				
1.3	**High Availability & Replication Options** *(Engine-native replication, active-passive/active-active cluster options, or proxy software)*	Per Core / Per Node				
1.4	**Enterprise Security & Compliance Options** *(Transparent Data Encryption (TDE), data masking, auditing, and vault security)*	Per Core / Per Instance				
1.5	**Centralized Management & Monitoring Software** *(Enterprise management consoles, diagnostic/tuning packs,*	Per Monitored Core				

Item	Component Description	Sizing Metric / Unit	Declared Sizing Metric	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
	operational monitoring tools)					
1.6	**Database Proxy / Load Balancing Platform** *(Virtual IP management, connection pooling, read/write splitting, query routing appliances or software)*	Per Core / Per Node				
1.7	Three (3) Years OEM 24/7 Enterprise Software Support & Maintenance	Lot				
1.8	Training for five (5) on the proposed database clustering and High Availability Solution At the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years KPC will provide Air Tickets, accommodation and out off pocket allowance for the delegates	PAX				
1.9	Any other item required to meet all the specifications in the Database and High Availability Services Compliance Matrix (Attach a list with price for each line item)					

4. **Database Infrastructure Sizing Declaration (Informational / Sizing Output for Infrastructure Team)- To fill by the tenderer**

This section carries $0 cost in this bid but forms a binding technical requirement for the separate Compute & Storage infrastructure provisioning.

Item	Component / Resource Type	Primary Site Sizing	DR Site Sizing	Total Sizing Declaration	Tenderer Comment
2.1	Total Allocated Compute (vCPU / Physical Cores)				
2.2	Total System Memory (RAM in GB) (Including dedicated in-memory allocation if applicable)				
2.3	Usable Storage Capacity (TB)				
2.4	Minimum Required Storage Performance *[Read/Write IOPS]*			[Peak Throughput MB/s]	

9E.7 Load Balancers/Application Delivery Controllers

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1	Application Delivery Controller (ADC) Appliances	4			
2	Centralized ADC Management Platform including Configuration Management, Analytics and Role-Based Administration	Lot			
3	ADC Configuration, Administration, Operations and Maintenance Training for 5No. Technical Team at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot			
4	Installation, Configuration and Integration with Datacenter Services	Lot			
5	All software licenses, subscriptions, and any other licenses required to fully meet all functional, operational, security, disaster recovery, high availability, and integration requirements specified in this tender document.	Lot			
6	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot			
7	Any other item required to meet all the specifications in the Load Balancing Platform Compliance Matrix (Attach a list with price for each line item)	Lot			

9E.8 Enterprise System Monitoring and Response Platform

Item	Description	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.	Enterprise System Monitoring and Response Platform inclusive of all modules required to meet specifications in Enterprise System Monitoring and Response Platform Compliance Matrix	Lot			
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all monitored objects	Lot			
3.	Administration, Operation and Maintenance Training for 5No. Administrators at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot			
4.	Minimum Three (3) Years 24x7x365 OEM Support, Updates Subscription, Security Patches and Firmware Updates	Years			
5.	All Licenses required to meet all the specifications in Enterprise System Monitoring and Response Platform Compliance Matrix	Lot			
6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)	Lot			

9E.9 Intrinsically Safe Tablets BOM

< Intentionally left blank>

9E.10 Terminal Management System (TMS) BOM

No.	TMS / Smart Loading Infrastructure Component	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1	**TMS Server and Compute Infrastructure**				
1.1	TMS Physical Enterprise Servers	**10**			
1.2	Server Operating System Licences	**10**			
1.3	TMS Database Platform	**5**			
1.4	Database High Availability / Replication	**5**			

No.	TMS / Smart Loading Infrastructure Component	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
1.5	Rack-Mounted TFT Administration Monitor	**5**			
2	**Queue Management Infrastructure**				
2.1	Outdoor Queue Display Screens (75-inch outdoor, IP65 – see Outdoor Queue Display Screens specification)	**30**			
3	**Driver and Vehicle Processing Infrastructure**				
3.1	RFID Readers (fixed, ultra-rugged; minimum quantity)	**30**			
3.2	RFIDs Chip – reusable tags for trucks (see Reusable UHF RFID Tags specification)	**150,000**			
3.3	RFID Printer / Encoder (see RFID Tag Printer specification)	**10**			
4	**Inspection and Field Device Infrastructure**				
4.1	ATEX Inspection Tablets / Mobile Devices and accessories (ATEX-rated, for MSOOS)	**40**			
5	**TMS Network and Communications Infrastructure**				
5.1	Fibre Optic Cabling	**2,100**			
5.2	Structured Network Cabling	**48 Dual Data points per site (5 sites)**			
5.3	Industrial Network Switches	**5No-48Ports**			
5.4	Secure IP Communication Components	**2 No. Next-Generation DC Firewall Appliances (HA pair at primary DC – see**			

No.	TMS / Smart Loading Infrastructure Component	Qty	Proposed OEM / Product	Proposed Tenderer Quantity	Tenderer Comments
		Firewall specification)			
5.5	Network Transceivers, SFPs and Optics	**30No. - 1G 30No. - 10G**			
5.6	Network Patch Cords and Accessories	**250No.-3m UTP Cables**			
6	**Other Required Infrastructure Components**	**Any other**			

9F Implementation Services BOM

9F.1 Work breakdown structure detailed BOM

The tenderer shall fill this Work breakdown structure detailed BOM with relevant Deliverable outputs and Acceptance criterion

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
1	**Project initiation**				
1.1	Project mobilisation	Project Initiation Report	1	Lot	
1.2	Project management plan	PMP	1	Document	
1.3	Governance establishment	Governance Charter/RACI	1	Lot	
1.4	Integrated project schedule	Baseline Schedule	1	Lot	
1.5	RAID framework	RAID Register	1	Lot	
2	**Requirements & Business Process**				
2.1	Business process discovery	Process Catalogue		Process	
2.2	As-Is assessment & Process Re-engineering	As-Is Process Maps		Process	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
2.3	To-Be design	To-Be Process Maps		Process	
2.4	Requirements validation	Requirements Catalogue		Requirement	
2.5	Fit-gap analysis	Fit-Gap Report		Module/Process	
2.6	Requirements baseline	Signed Requirements Baseline	1	Lot	
3	**Solution Architecture**				
3.1	Solution architecture	SAD	1	Lot	
3.2	Technical architecture	HLD/LLD	1	Lot	
3.3	Integration architecture	Integration Design	1	Lot	
3.4	Data architecture	Data Design	1	Lot	
3.5	Data Platform and Analytics Implementation				
3.6	Security architecture	Security Design	1	Lot	
4	**Functional Configuration**				
4.1	ERP Modules configuration	Configured Module		Module	
4.2	MSOOS Configurations				
4.3	TMS Configurations				
4.4	Workflow configuration	Configured Workflow		Workflow	
4.5	Role configuration	Security Roles		Role	
4.6	All Reporting configurations	Standard Reports		Report	
5	**Customisation / Development**				
5.1	Simple development	Development Object		Object	
5.2	Medium development	Development Object		Object	
5.3	Complex development	Development Object		Object	
5.4	Custom reports	Report		Report	
6	**Integration**				

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
6.1	Applications interface	Interface		Interface	
6.2	IT/OT interface	Interface		Interface	
6.3	External interface	Interface		Interface	
6.4	API development	API		API	
7	**Data Migration**				
7.1	Data profiling	Data Quality Report		Data Object	
7.2	Data mapping	Mapping Specification		Object	
7.3	Data cleansing	Cleansed Dataset		Object	
7.4	Mock migration 1	Migration Report	1	Cycle	
7.5	Mock migration 2	Migration Report	1	Cycle	
7.6	Mock migration 3	Migration Report	1	Cycle	
7.7	Production migration	Production Migration Report	1	Cycle	
8	**Infrastructure & Environments**				
8.1	Development environment	DEV	1	Environment	
8.2	Test environment	TEST	1	Environment	
8.3	UAT environment	UAT	1	Environment	
8.4	Production environment	PROD	1	Environment	
8.5	DR environment	DR	1	Environment	
9	**Cybersecurity & IAM**				
9.1	Role-Based Access Control (RBAC) Design & Implementation	Design and implement centralized RBAC	1	Report	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
9.2	Database & Application Security Controls	database and application controls	1	Report	
9.3	ERP Application Security Configuration & Hardening	Harden ERP application servers, application components	1	Report	
9.4	Security & Identity Integration Services	Integrate to SIEM, AD, PAM, SSO and MFA	1	Report	
9.5	Professional Integration Service for One Identity Solution	Professional Integration Service	1		
9.6	Security Documentation & Knowledge Transfer	Configuration documentation	Lot	Report	
9.7	Security Administration Certification Training for 5No staff	comprehensive OEM-authorized security training and certification	Lot	Training	
10	**Testing & QA**				
10.1	Test strategy	Test Strategy	1	Document	
	UT	UT Report	1	Document	
10.2	SIT	SIT Report	1	Phase	
10.3	Regression testing	Regression Report	1	Phase	
	Security Testing	Security Test Report	1	Document	
10.4	Performance testing	Performance Report	1	Phase	
10.5	UAT	UAT Report	1	Phase	
10.6	Cutover rehearsal	Rehearsal Report		Cycle	
11	**Change Management**				
11.1	Change impact assessment	Impact Report	1	Lot	
11.2	Stakeholder engagement	Engagement Programme	1	Lot	

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)
11.3	Business readiness	Readiness Report	1	Lot	
12	**Training & Knowledge Transfer**				
12.1	Training needs analysis	TNA	1	Lot	
12.2	End-user training	Training Sessions		Session	
12.3	Super-user training	Training Sessions		Session	
12.4	Technical training	Training Sessions		Session	
12.5	Administrator training	Training Sessions		Session	
13	**Cutover & Deployment**				
13.1	Cutover strategy	Strategy	1	Document	
13.2	Cutover plan	Cutover Plan	1	Document	
13.3	Go-live	Production Deployment	1	Event	
13.4	Rollback capability	Rollback Plan	1	Plan	
14	**Hypercare**				
14.1	Hypercare support – 6 Months	Support		Month	
14.2	Incident resolution	Incident		Incident	
15	**Handover & Closure**				
15.1	Operational handover	Handover Pack	1	Lot	
15.2	As-built documentation	As-Built Pack	1	Lot	
15.3	Lessons learned	Lessons Learned	1	Document	
15.4	Final project closure	Closure Report	1	Lot	
15.5	24 Months SLA	SLA Agreement	1	Lot	

9F.2 Tenderer Implementation services summary

WBS	Workstream	Fixed Price	Total Man-days
1	Project initiation & Mobilisation		
2	Requirements		
3	Architecture		
4	Configuration		
5	Development		
6	Integration		
7	Data and analytics platform		
8	Data Migration		
9	Infrastructure set-up		
10	Security		
11	Testing		
12	Change Management		
13	Training		
14	Cutover & Go-live		
15	Hypercare		
16	Support & Maintenance		
17	Handover/Closure		

9F.3 Resources for key positions

The tenderer shall populate and provide a schedule of **named resources for key positions** with costings indicating the WBS the resources shall support

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days
R03	Project Manager	Day-to-day management	8+ yrs				
R04	Solution Architect	Overall architecture	10+ yrs	Relevant			
R05	Enterprise Architect	Architecture governance	10+ yrs	Relevant			
R06	Functional Lead ERP	Functional delivery	8+ yrs	Product			
R06	Functional Lead MSOOS						
R07	Functional Lead Data						

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days
R08	Technical Lead	Technical delivery	8+ yrs	Product/Technical			
R09	Integration Lead	Interfaces/APIs	8+ yrs	Relevant			
R10	Data Migration Lead	Data migration	8+ yrs	Relevant			
R11	Security Lead	Security/IAM	8+ yrs	Security			
R12	Test Manager	QA/test governance	8+ yrs	ISTQB or equivalent			
R13	Change Manager	Change/adoption	8+ yrs	Relevant			
R14	Training Lead	Training/KT	5+ yrs	Relevant			
R15	Senior Developer	Development	5+ yrs	Product			
R16	Functional Consultant	Configuration	5+ yrs	Product			
R17	Technical Consultant	Technical implementation	5+ yrs	Product			

FORM OEM-IT: OEM AUTHORISATION LETTERS – Required for Lot 2: Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution Only

Where the Tenderer proposes to supply products of specific OEM brands, a separate OEM Authorisation Letter is required for each brand. Each letter shall:

i. Be on the OEM's official letterhead, signed by an authorised OEM representative;
ii. Name KPC PLC as the end-customer or authorise the Tenderer to submit a bid for this specific Tender;
iii. Confirm the Tenderer's current partnership/reseller/distributor status for the products proposed;
iv. Confirm that the products are genuine, new, non-end-of-life and eligible for OEM warranty support;
v. Be current (issued within the last 12 months or confirm ongoing validity).

OEM Authorisation Summary:

	Solution Domain	Proposed OEM / Technology Provider	Proposed Product / Solution	Authorisation Type *(OEM Direct / Authorised Partner / Certified Partner / Other)*	Authorisation Letter Attached (Yes/No)	Evidence Reference (Document / Page No.)
1.	Enterprise Resource Planning (ERP)					
2.	MSOOS					
3.	Enterprise Integration Platform / Middleware					
4.	Infrastructure (Servers and Storage)					
5.	Advanced Analytics inclusive of AI					

FORM COI-IT: CONFLICT OF INTEREST DECLARATION

I/We declare that: (1) No conflict of interest exists as defined in ITT Clause 4, OR (2) The following conflicts are disclosed [describe]. We did not participate in preparing the Technical Specifications/Terms of Reference for this tender. Any conflict of interest will be managed through the safeguards described.

Signed: _____ Date: _____ Title: _____

FORM BOD-IT: BENEFICIAL OWNERSHIP DISCLOSURE

No.	Full Name	Nationality	ID/Passport No.	% Owned	Nature of Control	Residence
1						
2						
3						

Listed company? State exchange: _____

Signed: _____ Date: _____

FORM ACD-IT: ANTI-CORRUPTION DECLARATION

I/We declare that: (1) No bribe, gift or inducement has been offered to KPC PLC employees; (2) We have not colluded with other Tenderers; (3) We comply with the Anti-Corruption and Economic Crimes Act 2003, Bribery Act 2016 and POCAMLA 2009; (4) Agents/intermediaries engaged [Name, Address, Fee]: [State 'None' if none].

Signed: _____ Date: _____ Seal: _____

FINANCIAL PROPOSAL FORMS — SUBMIT SEPARATELY IN SAP SRM PORTAL

The Financial Proposal forms below (FP-IT-1 through FP-IT-2) shall be submitted ONLY in the Financial Proposal workspace of the SAP SRM portal (or in a separately sealed physical envelope where applicable). Do NOT include any financial or cost information in the Technical Proposal.

FORM FP-IT-1: FINANCIAL PROPOSAL SUBMISSION FORM

Date: ____ Tender Ref: ____ We, [Firm Name], offer to supply [Project Title] for the total amount of:

Lot 1: Provision of Programme Management Office (PMO) Services: (Include Currency) _____ (excl. VAT)

VAT/ Applicable Taxes (state rate):

GRAND TOTAL (incl. VAT): (Include Currency) _____

Lot 2: Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution. (Include Currency) _____ (excl. VAT)

TOTAL CONTRACT VALUE — [Contract Period] 3 YEARS (excl. VAT): _____

VAT/ Applicable Taxes (state rate): (Include Currency S _____

GRAND TOTAL (incl. VAT): (Include Currency _____

Signed: ____ Date: ____

FORM FP-IT-2: BILL OF MATERIALS AND TOTAL COST SCHEDULE

All items listed in the Technical Bill of Materials must be costed and summarized into the various financial forms.

FORM FP-IT-2A: LOT 1 – PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES – BILL OF MATERIALS / PRICING SCHEDULE

It should at minimum cover:

No.	PMO Service	Description	Unit	Qty.	Unit Cost (USD)	Total Cost (USD)
1	**Programme Mobilisation and Initiation**	Programme Charter, governance framework, mobilisation plan, Integrated Master Programme Plan and Programme Management Plan	Lot	1		
2	**Programme Management and Coordination**	Coordination of programme workstreams, contractors, consultants, stakeholders and programme activities	Lot	1		
3	**Programme Planning and Controls**	Programme schedule, scope, cost, resource, performance and baseline management	Lot	1		
4	**Programme Governance**	Steering Committee support, governance meetings, decision tracking, action tracking and escalation management	Lot	1		
5	**Risk, Issue and Change Management**	Risk and issue registers, dependency management, change control and escalation	Lot	1		
6	**Contract and Contractor Performance Management**	Monitoring contractor deliverables, milestones, contractual obligations, performance and SLA compliance	Lot	1		
7	**Architecture and Design Oversight**	Review and oversight of solution architecture, technical designs and alignment with approved programme requirements	Lot	1		
8	**Implementation and Milestone Oversight**	Monitoring implementation progress, deliverables, milestones, stage gates and overall programme performance	Lot	1		
9	**Testing, Migration and Go-Live Oversight**	Oversight of testing, data migration, cutover, go-live readiness and stabilisation activities	Lot	1		

10	**Programme Reporting and Executive Support**	Programme dashboards, status reports, executive reports, performance reports and management presentations	Lot	1		
11	**Benefits Realisation Monitoring**	Benefits tracking, KPI monitoring, benefits reporting and alignment with programme objectives	Lot	1		
12	**Stakeholder and Communications Coordination**	Stakeholder coordination, programme communications, workshops and governance communications	Lot	1		
13	**Knowledge Transfer and Handover**	PMO knowledge transfer, programme records handover, lessons learned and transition support	Lot	1		
14	**Programme Closure**	Programme Closure Report, Benefits Realisation Report, Lessons Learned Report, Knowledge Transfer Completion Report and Final Handover Report	Lot	1		
15	**Other Required PMO Services**	Any additional PMO service necessary to achieve the requirements of Lot 1	Lot	1		
16	**SUBTOTAL**					
17	**APPLICABLE TAXES**					
	GRANDTOTAL – LOT 1 PMO SERVICES					

FORM FP-IT-2B: LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION – BILL OF MATERIALS

The Tenderer shall complete the following Priced Bill of Materials for all Components to successfully **Design, Supply, Install, Commission, Support and Maintain the proposed Enterprise Digital Solution.**

The Tenderer shall identify the proposed solution, OEM, licensing model, quantity, implementation requirements and applicable costs.

All Components listed in the priced BoM must meet the requirements and specification listed in the terms of reference contained in Section III of this tender document.

2B.1 Business Applications BOM

No.	Business Application / Capability	Proposed OEM / Product	Licensing Metric	KPC Baseline Quantity	Unit Cost (USD)	Total Cost (USD)
1.	Financial Operations		Users	300		
2.	Supply Chain Management		Users	893		
3.	Human Capital Management		Users	1,500		
4.	Payroll		Payroll Load	1,500		
5.	Enterprise Asset Management		Users	600		
6.	Project Lifecycle Management		Users	200		
7.	Strategic Planning and Performance Management		Users	100		
8.	Enterprise Risk Management		Users	100		
9.	Identity, access control, Multi-Factor and SSO		Users	1500		
10.	Customer Relationship Management (CRM)		Users	100		
11.	E - Procurement		Users	500		
12.	Contract Lifecycle Management (CLM)		Users	100		
13.	Sales and Commercial Management		Users	50		
14.	Safety Management		Users	1500		
15.	IT Service Management (ITSM)		Users	50		
16.	Enterprise Monitoring and Observability		Users	30		
17.	Integrated Development platform and workflow & Business Process Automation		Users(developers)	20		

No.	Business Application / Capability	Proposed OEM / Product	Licensing Metric	KPC Baseline Quantity	Unit Cost (USD)	Total Cost (USD)
18.	Integration platform		Integration Points	All Integration points		
19.	Comprehensive instructor-led certification training for 60No staff Functional Superuser ERP training Solution at OEM's authorized training center that has been in operation for atleast 5 years		Pax	60No		
20.	Include any other component necessary for the solution to meet all the functional and technical requirements.		LOT	LOT		
21.	Annual Maintenance if applicable		LOT			
	SUBTOTAL					
	APPLICABLE TAXES					
	GRAND TOTAL					

2B.2 Mid-Stream Oil Operations Solution and Terminal Management Solution BOM

i. The Tenderer shall provide a complete and fully itemized Bill of Materials for the Terminal Management System (TMS), Queue Management, Truck Inspection, Driver and Vehicle Management, Loading Operations and Loading Automation solution.

ii. The BOM shall include all software, licences, terminal equipment, TMS-specific site infrastructure, interfaces, integration components, implementation services, training, warranty, support and other components required to provide a complete and operational solution across the approved KPC loading terminals.

iii. The TMS shall support the five loading terminals identified in the Tender baseline: **PS09, PS10, PS25, PS27 and PS28**

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity	Unit Cost (USD)	Total Cost (USD)
1	**Order & Inventory Management**	Order management, inventory management, quantity conversion and standardisation	User / Enterprise	1 LOT			
2	**Nominations, Scheduling & Demand Forecasting**	Nominations, scheduling, allocation, capacity planning and demand forecasting	User / Enterprise	1 LOT			
3	**Terminal Management**	Terminal operations, truck/driver management, loading operations, loading station/arm management, gate and queue management	Terminal / Loading Station	1 LOT			
4	**Quality Control Management**	Product quality management, inspection, quality records and certificates	User / Enterprise	1 LOT			
5	**MSOOS Certification Training**	Comprehensive instructor-led certification training on 20No MSOOS Solution at OEM's authorized training center that has been in operation for atleast 5 years	Pax	20No			
6	**Other Required Components**	Any additional licences, modules, interfaces, middleware, software or	LOT	1			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity	Unit Cost (USD)	Total Cost (USD)
		services required for a complete solution					
	SUBTOTAL						
	APPLICABLE TAXES						
	GRAND TOTAL						

Notes

1. Quantities shall be validated through the approved site survey and detailed design for all applicable KPC locations.
2. The TMS shall cover all approved loading terminals.
3. The Tenderer shall provide all hardware, software, licences, interfaces, connectivity, cabling, accessories and other components required for a complete operational solution.
4. Existing KPC equipment proposed for reuse shall be clearly identified, and the Tenderer shall confirm compatibility and any required upgrades or modifications.
5. All implementation, configuration, integration, testing, commissioning, training, documentation, warranty and support costs shall be included in the relevant BOM items.
6. Recurring costs, including licences, subscriptions, connectivity and OEM support, shall be separately identified.
7. TMS-specific site and edge infrastructure shall be included in this BOM. Common enterprise data-centre infrastructure shall be priced under the **Infrastructure BOM** to avoid duplication.
8. The Tenderer shall provide OEM make/model, part numbers, licence SKUs and licensing metrics for all proposed components.
9. Where quantities are stated as **"As Required"**, the Tenderer shall provide the actual proposed quantity and shall not omit any component necessary to achieve the required functionality.
10. The Tenderer shall clearly distinguish **one-time costs, recurring costs, optional costs and future expansion costs**.

2B.3 Enterprise Data Analytics and AI BOM

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity	Unit Cost (USD)	Total Cost (USD)
1	**Enterprise Data & Analytics Platform**	Cloud data lake/Lakehouse, analytical platform, storage and processing capacity for 5 TB initial data with 10% annual growth	Subscription / Consumption	**1 LOT**			
2	**Data Integration & Data Engineering Platform**	ETL/ELT, API, CDC, batch and near-real-time integration, orchestration and data quality	Subscription / Consumption	**1 LOT**			
3	**Enterprise AI, Machine Learning, Data Science & Generative AI Platform**	AI/ML, data science, model development and MLOps, predictive and prescriptive analytics, forecasting, anomaly detection, Generative AI, natural-language analytics, intelligent recommendations and AI-assisted decision support	Subscription / Consumption	**1 LOT**			
4	**Data Governance, Security & Metadata Management**	Data catalogue, metadata, lineage, data quality, access control, audit, privacy and AI/ML governance	Subscription / Consumption	**1 LOT**			
5	**Power BI Integration**	Integration with KPC's existing Power BI environment, semantic models, analytical datasets, AI outputs and governed reporting data	Integration / LOT	**1**			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity	Unit Cost (USD)	Total Cost (USD)
6	**Enterprise Systems & External Data Integration**	Integration with ERP/Core System, TMS, EAM, HR, ITSM, operational systems, IoT/SCADA and approved external data sources	Integration / LOT	**1**			
7	**Cloud Infrastructure, HA, Backup & DR Services**	Compute, storage, network/data transfer, high availability, backup, disaster recovery, monitoring and security services	Subscription / Consumption	**1 LOT**			
8	**Implementation, Deployment & Priority AI/Analytics Use Cases**	Requirements validation, detailed solution architecture, platform configuration, data integration, testing, commissioning, and development/deployment of 5 agreed priority AI and advanced analytics use cases	LOT	**1**			
9	**Analytics/ML Certification Training**	Comprehensive instructor-led certification training on 12No AI/ML and analytics training Development at OEM's authorized training center that has been in operation for atleast 5 years	Pax	12No			
10	**Knowledge Transfer**	Administration, data engineering, data science, AI/ML and analytics training	Pax	**30 No**			
11	**Support, Maintenance, Updates &**	24×7 support, platform maintenance, software updates,	Annual Subscription	**5 Years**			

No.	Component	Description	Licensing / Pricing Metric	KPC Baseline Quantity	Tenderer Proposed Quantity	Unit Cost (USD)	Total Cost (USD)
	Technical Assistance	security patches, upgrades and technical assistance					
12	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**			
	SUBTOTAL						
	APPLICABLE TAXES						
	GRAND TOTAL						

2B.4 Enterprise Middleware & Application Development Platform BOM

No.	BOM Component	Description / Scope	License Metric	Estimated Qty.	Tenderer Proposed Quantity	Unit Price (USD)	Total Price (USD)
1	**Integration Platform**	Core middleware / integration platform	Lot	1			
2	**API Management Platform**	API publishing, lifecycle management and governance	Lot	1			
3	**Enterprise Service Bus (ESB)**	Service orchestration and application integration	Lot	1			
4	**Message Broker**	Asynchronous messaging and event distribution	Lot	1			
5	**Event Streaming Platform**	Real-time event streaming and processing	Lot	1			
6	**Workflow / Orchestration Engine**	Process orchestration across systems	Lot	1			
7	**Data Transformation Engine**	Mapping, transformation and enrichment	Lot	1			

8	**Integrations and Application Development Certification**	Comprehensive instructor-led certification training on 15No Integrations and Application Development at OEM's authorized training center that has been in operation for atleast 5 years	Pax	15No			
9	**Other Required Components**	Any additional licences, subscriptions, services or components required to provide a complete operational solution	LOT	**1**			
	Subtotal						
	Applicable Taxes						
	Grand Total						

2B.5 Infrastructure BOM

2B.5A Compute Platform

iii. Compute Platform – Primary Site

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
1.	Enterprise x86 Rack Servers	6		
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot		
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot		
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot		
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
6.	Comprehensive instructor-led certification training on operating system and security administration, virtualization,	5		

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
	containerization, database and performance tuning Training for Proposed Compute Platform for 5No. System Administrators at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates			
7.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.			
	Subtotal			
	Applicable Taxes			
	Grand Total			

iv. Compute Platform – DR Site

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
1.	Enterprise x86 Rack Servers	4		
2.	Adapters, Transceivers, Optics, Cabling, and Connectivity components	Lot		
3.	All In-inclusive Software & Management License Bundles (3) Years	Lot		
4.	Three (3) Years Hardware, Hypervisors, Virtualization, Containerization, Operating System and all other licenses applicable for successful setup of the compute and storage infrastructure	Lot		
5.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
6.	Any other component required for digital transformation solution to be implemented and operated within performance metrics.			
	Subtotal			
	Applicable Taxes			
	Grand Total			

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements including performance metrics.
3. No additional licenses or subscriptions required for full functionality shall be excluded from the BOQ.
4. All required adapters, transceivers, optics, cabling, and connectivity components shall be included to meet the specified connectivity and performance requirements.

5. Support shall cover a minimum period of three (3) years.
6. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2B.5B New Enterprise Storage

i. New Enterprise Storage - Primary Site

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
1.	All-NVMe Unified Storage Array	1		
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2		
3.	Controller Memory Cache (Minimum 384GB per controller, 768GB per array)	Included		
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included		
5.	NVMe TLC SSDs configured to deliver minimum 115TB usable capacity per array before data reduction	1 Lot		
6.	Rack Mounting Kits and Accessories	Included		
7.	Enterprise All-Inclusive Storage Software License Bundle covering all licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems	Lot		
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of Primary Storage Systems.	Lot		
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
10	Comprehensive instructor-led Storage Implementation, Administration, Operation, Security, Maintenance and Troubleshooting Training for Five (5) ICT Personnel at the Original Equipment Manufacturer's Approved Training Center that has been in operation for atleast 5 years. KPC will provide Air Ticket, accommodation and out off pocket allowance for the delegates	Lot		
11	Any other component required for the successful implementation of the Enterprise digital solution			
	Subtotal			

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
	Applicable Taxes			
	Grand Total			

ii. New Unified Enterprise All NVMe – DR Site

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
1.	All-NVMe Unified Storage Array	1		
2.	Storage Controllers (Minimum 64 CPU Cores @ ≥2.0GHz per array)	2		
3.	Controller Memory Cache (Minimum 256GB per controller, 512GB per array)	Included		
4.	NVRAM/SCM Cache Modules for Hot Data Acceleration and Burst Workloads	Included		
5.	NVMe TLC SSDs configured to deliver minimum **70TB usable capacity** per array before data reduction	Lot		
6.	Rack Mounting Kits and Accessories	Included		
7.	Enterprise All-Inclusive Storage Software License Bundle covering all licensed features and functionalities required under this tender for both Primary and Disaster Recovery (DR) storage systems	Lot		
8.	Installation, Configuration, Replication Setup, Migration Support, Disaster Recovery Testing, Documentation, and Commissioning of DR Storage Systems.	Lot		
9.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
10	Any other component required for the successful implementation of the Enterprise digital solution			
	Subtotal			
	Applicable Taxes			
	Grand Total			

Notes:

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. All SAN switches shall be supplied by the same manufacturer as the proposed storage solution.
4. All licenses required for operation, management, monitoring, diagnostics, analytics, trunking, and future port activation shall be included.
5. The solution shall support dual-fabric deployment across both Primary and Disaster Recovery sites.
6. Support subscriptions shall cover a minimum period of three (3) years.
7. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2B.5C Storage Expansion For Existing Dell EMC Unity XT 480 Storage Arrays

Item No.	Description	Unit	Qty	Unit Price (USD)	Total Price (USD)
1.	Dell EMC Unity XT 480 compatible expansion shelves including all required power supplies, fans, SAS cables, rail kits and installation accessories required for complete installation	Lot			
2.	SSD capacity expansion delivering a minimum of **20 TB usable capacity** configured in RAID 5 in Primary Site	Lot			
3.	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in Primary Site	Lot			
4.	NL-SAS capacity expansion delivering a minimum of **100 TB usable capacity** configured in RAID 6 in Primary Site	Lot			
5.	SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot			
6.	NL-SAS capacity expansion delivering a minimum of **50 TB usable capacity** configured in RAID 6 in DR Site	Lot			
7.	All licenses required to support the expanded capacity including snapshots, thin clones, replication, QoS, storage management,	Lot			

Item No.	Description	Unit	Qty	Unit Price (USD)	Total Price (USD)
	performance monitoring and data reduction features				
8.	Installation, configuration, testing, commissioning and integration services	Lot			
9.	Minimum Three (3) years OEM hardware and software support, including firmware updates and technical support	Lot			
10	Any other item required to complete works/project				
	Subtotal				
	Applicable Taxes				
	Grand Total				

Tenderers to disclose how they achieved the capacity in table below.

Site	Storage Tier	RAID Type	Required Usable Capacity	Proposed Drive Size	Proposed Number of Drives	Raw Capacity	Usable Capacity
Primary	SSD	RAID 5	20 TB				
	SAS	RAID 6	50 TB				
	NL-SAS	RAID 6	100 TB				
DR	SAS	RAID 6	50 TB				
	NL-SAS	RAID 6	50 TB				

Notes

5. The proposed solution is intended for the expansion of KPC's existing Dell EMC Unity XT 480 storage arrays and not for replacement of the existing systems.
6. All proposed hardware, software, drives, licenses, enclosures, cables, transceivers, drive carriers, mounting kits, and ancillary components required to achieve the specified capacities and maintain full OEM support shall be included in the tenderer's proposal even if not expressly listed in this BOQ.
7. All capacities quoted shall be usable capacities after RAID configuration and shall exclude system overheads unless otherwise stated.
8. The implementation shall be completed without disruption to production services and without requiring replacement of the existing storage arrays.

2B.5D SAN Switches

i. SAN Switches - Primary Site

Item	Description	Qty	Unit Price(USD)	Total Price(USD)
1.	64-Port 64Gbps Enterprise SAN Switch	2		
2.	64Gbps FC SFP56 Transceivers	64		
3.	OM4 LC-LC Duplex Patch Cords (3m)	20		

4.	Rack Mounting Kits and Accessories	Lot		
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot		
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot		
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance and Troubleshooting Training for Five (5) System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot		
9.	Any other component required for the successful implementation of the Enterprise digital solution			
	Subtotal			
	Applicable Taxes			
	Grand Total			

ii. SAN Switches – DR Site

Item	Description	Qty	Unit Price(USD)	Total Price(USD)
1.	64-Port 64Gbps Enterprise SAN Switch	2		
2.	64Gbps FC SFP56 Transceivers	64		
3.	OM4 LC-LC Duplex Patch Cords (3m)	20		
4.	Rack Mounting Kits and Accessories	Lot		
5.	SAN Switch Software and Feature Licenses (all-inclusive)	Lot		
6.	Installation, Configuration, Zoning, Integration, Testing and Commissioning	Lot		
7.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
8.	Comprehensive instructor-led Foundational and Advanced SAN Switch Administration, Maintenance	Lot		

	and Troubleshooting Training for Five (5) System Administrators onsite.			
9.	Any other component required for the successful implementation of the Enterprise digital solution			
	Subtotal			
	Applicable Taxes			
	Grand Total			

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. Quantities of transceivers and patch cords are minimum requirements based on 32 active ports per switch.
4. All SAN switches shall be supplied by the same manufacturer as the proposed storage solution.
5. All licenses **required** for the operation of the proposed solution, including activated ports, fabric services, diagnostics, monitoring, management, and trunking, shall be included. The proposed switch shall support future port activation through software licensing without hardware replacement.
6. The solution shall support dual-fabric deployment across both Primary and Disaster Recovery sites.
7. Support shall cover a minimum period of three (3) years.
8. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2B.5E Cloud Automation and Orchestration Platform

Item	Description	Qty	Unit Price	Total Price
1.	Cloud Automation and Orchestration Platform for centralized management, orchestration, monitoring, automation, and lifecycle management of all proposed Servers, Storage systems, SAN infrastructure, network infrastructure, and related components.	Lot		
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all proposed infrastructure assets into the platform.	Lot		
3.	Administration, Operation and Maintenance Training for 5No. System Administrators at OEM's authorized training center that has been in operation for atleast 5 years	Lot		
4.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Years		
5.	All Licenses required to meet all the Cloud Automation and Orchestration Platform specifications			

6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)			
	Subtotal			
	Applicable Taxes			
	Grand Total			

Notes

1. Pricing shall include all licenses, subscriptions, software components, connectors, agents, implementation services, training, documentation, and support necessary to meet all mandatory Cloud Automation and Orchestration Platform requirements.
2. No additional software, licenses, subscriptions, or modules shall be required to achieve full compliance with the Cloud Automation and Orchestration Platform requirements.
3. All prices shall include at least three (3) years of software subscription, updates, security patches, and 24x7 OEM support.

2B.5F Database and High Availability Infrastructure

Database Engine & Platform Software Licensing

Item	Component Description	Sizing Metric / Unit	Declared Sizing Metric	Unit Price	Total Price
1.1	**Core Enterprise Database Software Licenses** *(Base engine licenses required to support primary and HA/DR workloads based on Tenderer's sizing)*	Per Core / Per CPU			
1.2	**In-Memory / Advanced Performance Options** *(In-memory, columnar, or partitioning add-ons required for full workload throughput)*	Per Core / Per RAM GB			
1.3	**High Availability & Replication Options** *(Engine-native replication, active-passive/active-active cluster options, or proxy software)*	Per Core / Per Node			
1.4	**Enterprise Security & Compliance Options** *(Transparent Data Encryption (TDE), data masking, auditing, and vault security)*	Per Core / Per Instance			
1.5	**Centralized Management & Monitoring Software** *(Enterprise management consoles, diagnostic/tuning packs, operational monitoring tools)*	Per Monitored Core			

Item	Component Description	Sizing Metric / Unit	Declared Sizing Metric	Unit Price	Total Price
1.6	**Database Proxy / Load Balancing Platform** *(Virtual IP management, connection pooling, read/write splitting, query routing appliances or software)*	Per Core / Per Node			
1.7	Three (3) Years OEM 24/7 Enterprise Software Support & Maintenance	Lot			
1.8	Training for five (5) on the proposed database clustering and High Availability Solution At the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years KPC will provide Air Tickets, accommodation and out off pocket allowance for the delegates				
1.9	Any other item required to meet all the specifications in the Database and High Availability Services Compliance Matrix (Attach a list with price for each line item)				
	Subtotal				
	Applicable Taxes				
Grand Total					

1. Database Infrastructure Sizing Declaration (Informational / Sizing Output for Infrastructure Team)- To fill by the tenderer				
This section carries $0 cost in this bid but forms a binding technical requirement for the separate Compute & Storage infrastructure provisioning.				
Item	**Component / Resource Type**	**Primary Site Sizing**	**DR Site Sizing**	**Total Sizing Declaration**
2.1	Total Allocated Compute (vCPU / Physical Cores)			
2.2	Total System Memory (RAM in GB) (Including dedicated in-memory allocation if applicable)			
2.3	Usable Storage Capacity (TB)			

2.4	Minimum Required Storage Performance*[Read/Write IOPS]*			[Peak Throughput MB/s]

Note:

1. Licensing Metrics: Tenderers must explicitly state their licensing model (e.g., Per Core, Per Processor, or Per User/Socket)
2. Engine-Specific Options: Tenderers proposing specialized appliances or engineered systems may bundle hardware and software line items, provided the hardware and OEM support components are clearly broken down.
3. Tenderers must guarantee that the total licensed cores listed above are sufficient to deliver the target performance, RPO, and RTO on the shared infrastructure.
4. Sizing Liability Clause: Tenderers are required to perform comprehensive workload sizing based on the transaction volumes, database sizes, and five years growth rate.
5. The software licenses priced in Section 1 must fully support the declared infrastructure requirements in Section 2. If, during implementation or commissioning, the proposed software core licenses prove insufficient to meet the performance SLAs, RPO, or RTO due to tenderer under sizing, the tenderer shall supply all additional required software licenses and OEM support at no additional cost to the Corporation.

2B.5G Load Balancers/Application Delivery Controllers

Item	Description	Qty	Unit Price (USD)	Total Price (USD)
1.	Application Delivery Controller (ADC) Appliances	4		
2.	Centralized ADC Management Platform including Configuration Management, Analytics and Role-Based Administration	Lot		
3.	ADC Configuration, Administration, Operations and Maintenance Training for 5No. Technical Team at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot		
4.	Installation, Configuration and Integration with Data Center Services	Lot		
5.	All software licenses, subscriptions, and any other licenses required to fully meet all functional, operational, security, disaster recovery, high availability, and integration requirements specified in this tender document.	Lot		
6.	Minimum Three (3) Years 24x7x365 OEM Hardware & Software Support, Updates Subscription, Security Patches and Firmware Updates	Lot		
7.	Any other item required to meet all the specifications in the Load Balancing Platform Compliance Matrix (Attach a list with price for each line item)			
	Subtotal			
	Applicable Taxes			
	Grand Total			

Notes

1. Prices shall be inclusive of delivery, installation, configuration, testing, commissioning and documentation.
2. Prices shall include all hardware, software, licenses, subscriptions and professional services required to meet all requirements.
3. No additional licenses or subscriptions required for full functionality shall be excluded from the BOQ.
4. Support subscriptions shall cover a minimum period of three (3) years.
5. Vendor shall indicate OEM product model, part numbers and license SKUs against each BOQ line item in the proposal.

2B.5H Enterprise System Monitoring and Response Platform

Item	Description	Qty	Unit Price	Total Price
1.	Enterprise System Monitoring and Response Platform inclusive of all modules required to meet specifications in Enterprise System Monitoring and Response Platform Compliance Matrix	Lot		
2.	Installation, configuration, integration, testing, commissioning, and onboarding of all monitored objects	Lot		
3.	Administration, Operation and Maintenance Training for 5No. Administrators at the Original Equipment Manufacturer's Approved Training Centre that have been operation for 5 years	Lot		
4.	Minimum Three (3) Years 24x7x365 OEM Support, Updates Subscription, Security Patches and Firmware Updates	Years		
5.	All Licenses required to meet all the specifications in Enterprise System Monitoring and Response Platform Compliance Matrix			
6.	Any other item required to meet all the specifications in the Cloud Automation and Orchestration Platform Compliance Matrix (Attach a list with price for each line item)			
	Subtotal			
	Applicable Taxes			
	Grand Total			

2B.5I Intrinsically Safe Tablets BOM

<Intentionally left blank>

2B.5J Terminal Management System (TMS) BOM

No.	TMS / Smart Loading Infrastructure Component	Qty	Unit Price (USD)	Total Price (USD)
1	**TMS Server and Compute Infrastructure**			
1.1	TMS Physical Enterprise Servers	**10**		
1.2	Server Operating System Licences	**10**		
1.3	TMS Database Platform	**5**		
1.4	Database High Availability / Replication	**5**		
1.5	Rack-Mounted TFT Administration Monitor	**5**		
2	**Queue Management Infrastructure**			
2.1	Outdoor Queue Display Screens (75-inch outdoor, IP65 – see Outdoor Queue Display Screens specification)	**30**		
3	**Driver and Vehicle Processing Infrastructure**			
3.1	RFID Readers (fixed, ultra-rugged; minimum quantity)	**30**		
3.2	RFIDs Chip – reusable tags for trucks (see Reusable UHF RFID Tags specification)	**150,000**		
3.3	RFID Printer / Encoder (see RFID Tag Printer specification)	**10**		
4	**Inspection and Field Device Infrastructure**			
4.1	ATEX Inspection Tablets / Mobile Devices and accessories (ATEX-rated, for MSOOS)	**40**		
5	**TMS Network and Communications Infrastructure**			

No.	TMS / Smart Loading Infrastructure Component	Qty	Unit Price (USD)	Total Price (USD)
5.1	Fibre Optic Cabling	**2,100**		
5.2	Structured Network Cabling	**48 Dual Data points per site (5 sites)**		
5.3	Industrial Network Switches	**5No-48Ports**		
5.4	Secure IP Communication Components	**2 No. Next-Generation DC Firewall Appliances (HA pair at primary DC – see Firewall specification)**		
5.5	Network Transceivers, SFPs and Optics	**30No. - 1G 30No. - 10G**		
5.6	Network Patch Cords and Accessories	**250No.-3m UTP Cables**		
6	**Other Required Infrastructure Components**	**Any Other**		

2B.6 Implementation Services BOM

2B.6A Work breakdown structure detailed BOM

The tenderer shall fill this Work breakdown structure detailed BOM with relevant Deliverable outputs and Acceptance criterion

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
1	**Project initiation**						
1.1	Project mobilisation	Project Initiation Report	1	Lot			
1.2	Project management plan	PMP	1	Document			
1.3	Governance establishment	Governance Charter/RACI	1	Lot			

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
1.4	Integrated project schedule	Baseline Schedule	1	Lot			
1.5	RAID framework	RAID Register	1	Lot			
2	**Requirements & Business Process**						
2.1	Business process discovery	Process Catalogue		Process			
2.2	As-Is assessment & Process Re-engineering	As-Is Process Maps		Process			
2.3	To-Be design	To-Be Process Maps		Process			
2.4	Requirements validation	Requirements Catalogue		Requirement			
2.5	Fit-gap analysis	Fit-Gap Report		Module/Process			
2.6	Requirements baseline	Signed Requirements Baseline	1	Lot			
3	**Solution Architecture**						
3.1	Solution architecture	SAD	1	Lot			
3.2	Technical architecture	HLD/LLD	1	Lot			
3.3	Integration architecture	Integration Design	1	Lot			
3.4	Data architecture	Data Design	1	Lot			
3.5	Data Platform and Analytics Implementation						
3.6	Security architecture	Security Design	1	Lot			
4	**Functional Configuration**						
4.1	ERP Modules configuration	Configured Module		Module			

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
4.2	MSOOS Configurations						
4.3	TMS Configurations						
4.4	Workflow configuration	Configured Workflow		Workflow			
4.5	Role configuration	Security Roles		Role			
4.6	All Reporting configurations	Standard Reports		Report			
5	**Customisation / Development**						
5.1	Simple development	Development Object		Object			
5.2	Medium development	Development Object		Object			
5.3	Complex development	Development Object		Object			
5.4	Custom reports	Report		Report			
6	**Integration**						
6.1	Applications interface	Interface		Interface			
6.2	IT/OT interface	Interface		Interface			
6.3	External interface	Interface		Interface			
6.4	API development	API		API			
7	**Data Migration**						
7.1	Data profiling	Data Quality Report		Data Object			
7.2	Data mapping	Mapping Specification		Object			
7.3	Data cleansing	Cleansed Dataset		Object			
7.4	Mock migration 1	Migration Report	1	Cycle			
7.5	Mock migration 2	Migration Report	1	Cycle			
7.6	Mock migration 3	Migration Report	1	Cycle			

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
7.7	Production migration	Production Migration Report	1	Cycle			
8	**Infrastructure & Environments**						
8.1	Development environment	DEV	1	Environment			
8.2	Test environment	TEST	1	Environment			
8.3	UAT environment	UAT	1	Environment			
8.4	Production environment	PROD	1	Environment			
8.5	DR environment	DR	1	Environment			
9	**Cybersecurity & IAM**						
9.1	Role-Based Access Control (RBAC) Design & Implementation	Design and implement centralized RBAC	1	Report			
9.2	Database & Application Security Controls	database and application controls	1	Report			
9.3	ERP Application Security Configuration & Hardening	Harden ERP application servers, application components	1	Report			
9.4	Security & Identity Integration Services	Integrate to SIEM, AD,PAM, SSO and MFA	1	Report			
9.5	Professional Integration Service for One Identity Solution	Professional Integration Service	1				
9.6	Security Documentation &	Configuration documentation	Lot	Report			

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
	Knowledge Transfer						
9.7	Security Administration Certification Training for 5No staff	comprehensive OEM-authorized security training and certification	Lot	Training			
10	**Testing & QA**						
10.1	Test strategy	Test Strategy	1	Document			
	UT	UT Report	1	Document			
10.2	SIT	SIT Report	1	Phase			
10.3	Regression testing	Regression Report	1	Phase			
	Security Testing	Security Test Report	1	Document			
10.4	Performance testing	Performance Report	1	Phase			
10.5	UAT	UAT Report	1	Phase			
10.6	Cutover rehearsal	Rehearsal Report		Cycle			
11	**Change Management**						
11.1	Change impact assessment	Impact Report	1	Lot			
11.2	Stakeholder engagement	Engagement Programme	1	Lot			
11.3	Business readiness	Readiness Report	1	Lot			
12	**Training & Knowledge Transfer**						
12.1	Training needs analysis	TNA	1	Lot			
12.2	End-user training	Training Sessions		Session			
12.3	Super-user training	Training Sessions		Session			
12.4	Technical training	Training Sessions		Session			
12.5	Administrator training	Training Sessions		Session			
13	**Cutover & Deployment**						

WBS	Activity	Deliverable / Output	Quantity	Unit	Effort (Man-Days)	Unit Rate (USD)	Total Price (USD)
13.1	Cutover strategy	Strategy	1	Document			
13.2	Cutover plan	Cutover Plan	1	Document			
13.3	Go-live	Production Deployment	1	Event			
13.4	Rollback capability	Rollback Plan	1	Plan			
14	**Hypercare**						
14.1	Hypercare support – 6 Months	Support		Month			
14.2	Incident resolution	Incident		Incident			
15	**Handover & Closure**						
15.1	Operational handover	Handover Pack	1	Lot			
15.2	As-built documentation	As-Built Pack	1	Lot			
15.3	Lessons learned	Lessons Learned	1	Document			
15.4	Final project closure	Closure Report	1	Lot			
15.5	24 Months SLA	SLA Agreement	1	Lot			
	SUBTOTAL						
	APPLICABLE TAXES						
	GRAND TOTAL						

2B.6B Tenderer Implementation services summary

WBS	Workstream	Fixed Price	Total Man-days	Total Bid Price
1	Project initiation & Mobilisation			
2	Requirements			
3	Architecture			
4	Configuration			
5	Development			
6	Integration			
7	Data and analytics platform			
8	Data Migration			
9	Infrastructure set-up			
10	Security			
11	Testing			
12	Change Management			
13	Training			
14	Cutover & Go-live			
15	Hypercare			
16	Support & Maintenance			
17	Handover/Closure			
	SUBTOTAL			
	APPLICABLE TAXES			
	GRAND TOTAL			

2B.6C Resources for key positions

The tenderer shall populate and provide a schedule of **named resources for key positions** with costings indicating the WBS the resources shall support

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days	Daily Rate	Total Cost	WBS Supported
R03	Project Manager	Day-to-day management	8+ yrs							All
R04	Solution Architect	Overall architecture	10+ yrs	Relevant						
R05	Enterprise	Architecture	10+ yrs	Relevant						

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days	Daily Rate	Total Cost	WBS Supported
	Architect	governance								
R06	Functional Lead ERP	Functional delivery	8+ yrs	Product						
R06	Functional Lead MSOOS									
R07	Functional Lead Data									
R08	Technical Lead	Technical delivery	8+ yrs	Product/Technical						
R09	Integration Lead	Interfaces/APIs	8+ yrs	Relevant						
R10	Data Migration Lead	Data migration	8+ yrs	Relevant						
R11	Security Lead	Security/IAM	8+ yrs	Security						
R12	Test Manager	QA/test governance	8+ yrs	ISTQB or equivalent						
R13	Change Manager	Change/adoption	8+ yrs	Relevant						
R14	Training Lead	Training/KT	5+ yrs	Relevant						
R15	Senior Developer	Development	5+ yrs	Product						
R16	Functional Consultant	Configuration	5+ yrs	Product						
R17	Technical	Technical implementation	5+ yrs	Product						

ID	Role	Responsibility	Experience	Certification	Named Resource	Allocation %	Man-Days	Daily Rate	Total Cost	WBS Supported
	Consultant									

2B.6D Consultant Rate card

Role	Hourly Rate	Daily Rate	Weekly Rate	Monthly Rate	Overtime Rate	Weekend Rate	Travel Day Rate
Project Manager							
Solution Architect							
Functional Consultants							
Technical Consultant							
Developer							
Integration Specialist							
Data Specialist							
Security Specialist							
Test Specialist							
Change Manager							
Trainer							

PART 3 – EVALUATION FRAMEWORK

SECTION IV: IT PROCUREMENT EVALUATION FRAMEWORK

KPC PLC evaluates IT tenders using a rigorous, structured, multi-stage process designed for the specific characteristics of IT procurement — where solution quality, security, vendor viability, implementation capability and lifecycle cost are equally important as the quoted price. No criteria, methods or factors other than those in this Section shall be used in evaluation.

B. STAGE 1 — PRELIMINARY / ADMINISTRATIVE REVIEW (PASS/FAIL)

Tenders failing any mandatory requirement shall be rejected at Stage 1 without proceeding to technical evaluation:

No.	Mandatory Requirement	Pass / Fail
1.	Form TP-IT-1A: Technical Proposal Submission Form — signed	*PASS / FAIL*
2.	Form TP-IT-1B: Consortium Agreement form- Signed by all parties where appliable	*PASS / FAIL*
3.	Form TP-IT-2: Tenderer Profile and Experience — completed	*PASS / FAIL*
4.	Form TP-IT-3: Technical Solution Description — provided for Lot 2 Only	*PASS / FAIL*
5.	Form TP-IT-4: Technical Compliance Matrix — completed for all requirements	*PASS / FAIL*
6.	Form TP-IT-5: Implementation Plan — provided	*PASS / FAIL*
7.	Form TP-IT-6: Proposed Team and CVs — provided	*PASS / FAIL*
8.	Form TP-IT-7: SLA Proposal — provided for Lot 2 Only	*PASS / FAIL*
9.	Form TP-IT-8: Cybersecurity and Data Protection Declaration — signed	*PASS / FAIL*
10.	Form TP-IT-9: Technical Bill of Material — signed	*PASS / FAIL*
11.	Form OEM-IT: OEM Authorisation Letters — provided for all specified brands for Lot 2 Only	*PASS / FAIL*
12.	Form COI-IT: Conflict of Interest Declaration — signed	*PASS / FAIL*
13.	Form BOD-IT: Beneficial Ownership Disclosure — completed	*PASS / FAIL*
14.	Form ACD-IT: Anti-Corruption Declaration — signed	*PASS / FAIL*
15.	Tender Security — provided	*PASS / FAIL*
16.	Valid KRA Tax Compliance Certificate (Kenyan firms)	*PASS / FAIL*
17.	Certificate of Incorporation / Business Registration	*PASS / FAIL*
18.	Tender submitted by the submission deadline	*PASS / FAIL*
19.	Tender valid for the required period stated in the Data Sheet	*PASS / FAIL*

20.	Satisfactory performance as per KPC's contractor appraisal records, or without contract termination, or notice of termination, or notice of non-performance or delays issued against them.	*PASS / FAIL*

C. STAGE 2 — TECHNICAL COMPLIANCE REVIEW (PASS/FAIL)

Technical compliance review shall be done in two stages. The first stage shall involve reviewing whether the tenderer meets the below set minimum criteria.

LOT 1: PROVISION OF PROGRAMME MANAGEMENT OFFICE (PMO) SERVICES

MANDATORY REQUIREMENTS

Ref	Item	Description	Evidence Required	Pass/Fail
1	Audited Financial Statements	The respondent shall demonstrate sound financial capacity to undertake the assignment.	Audited financial statements for the last three (3) financial years.	
2	Minimum Annual Turnover	The respondent shall have an average annual turnover of not less than **USD 1 million** over the last three (3) financial years.	Audited financial statements or an auditor's certificate confirming annual turnover.	
3	Financial Stability	The respondent shall have maintained a positive net worth during the last three (3) financial years.	Audited financial statements.	
4	Financial Capability	The respondent shall demonstrate access to sufficient financial resources to undertake the assignment.	Bank reference letter issued within the last six (6) months by the respondent's principal banker.	
5	Programme Management Experience	The respondent shall have successfully completed at least three (3) Programme Management Office (PMO) or programme management assignments of comparable scope and complexity within the last seven (7) years.	Completion certificates or client reference letters indicating scope, value, and completion status.	

Ref	Item	Description	Evidence Required	Pass/Fail
6	ERP / Digital Transformation Experience	The respondent shall have successfully managed at least two (2) enterprise ERP or digital transformation programmes within the last ten (10) years.	Completion certificates, client reference letters, or signed contracts.	
7	Industry Experience	The respondent shall have completed at least two (2) assignments for midstream oil and gas operators (pipelines and terminals) or comparable asset-intensive organisations in the energy, utilities, transport, logistics, or manufacturing sectors.	Completion certificates, client reference letters, or signed contracts.	
8	Multi-Vendor Programme Management	The respondent shall demonstrate experience managing programmes involving multiple implementation vendors and integrated solution delivery.	Project descriptions, client references, or completion certificates.	
9	Client References	The respondent shall provide at least three (3) contactable client references for the similar assignments submitted. The three projects should each be above USD 1 Million in value.	Client reference letters containing contact details of the client representative.	
10	Programme Management Methodology	The respondent shall have an established programme and project management methodology.	Methodology documentation or sample governance framework.	
11	Information Security	The Respondent shall maintain and operate an Information Security	Valid ISO/IEC 27001 certificate or equivalent for PMO	

Ref	Item	Description	Evidence Required	Pass/Fail
		Management System (ISMS) appropriate to the provision of the goods and services under this tender.		
12	Programme Director / PMO Lead	Bachelor's Degree in ICT, Engineering, Business, Project Management or related discipline; PMP, PRINCE2 Practitioner, MSP or equivalent certification; minimum fifteen (15) years' experience; and successful leadership of at least three (3) enterprise digital transformation programmes.	Curriculum Vitae, academic certificates, professional certifications, and project references.	
13	Business Process Transformation Lead	Degree in Business, Engineering, ICT or related discipline; Lean Six Sigma or equivalent certification; minimum eight (8) years' experience in business process transformation in the private sector.	Curriculum Vitae, academic certificates, professional certifications, and project references.	
14	Change Management Lead	Degree in Human Resources, Business or related discipline; Prosci (ADKAR) or equivalent certification; minimum eight (8) years' experience in organizational change management.	Curriculum Vitae, academic certificates, professional certifications, and project references.	
15	PMO Controls / Planning Specialist	Degree in a relevant discipline; minimum seven (7) years' experience in programme planning and controls.	Curriculum Vitae, academic certificates, professional certifications, and project references.	

Ref	Item	Description	Evidence Required	Pass/Fail
16	Risk & Benefits Realisation Specialist	Degree in a relevant discipline; recognised risk management qualification; minimum seven (7) years' experience in enterprise risk and benefits management.	Curriculum Vitae, academic certificates, professional certifications, and project references.	

LOT 2: DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION

MANDATORY REQUIREMENTS

Solution Requirements (MR-S01 to MR-S18)

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-S01	The tenderer, or the consortium member responsible for the ERP, holds current OEM partnership status with an ERP.	ERP partnership record and an OEM letter of authorisation for this tender.	
MR-S02	The offered ERP edition is deployed on-premises or in an in-country cloud, at a release in OEM mainstream maintenance at go-live.	Product schedule naming edition, release and activated industry business functions	
MR-S03	At least three (3) completed implementations, in the last ten (10) years, for oil and gas operators using the proposed MSOOS. The clients must have a similar operating model to KPC.	Client reference letters with contact, scope, go-live date and the tenderer's role	
MR-S04	At least one (1) completed conversion from SAP ECC 6.0 to the proposed ERP, in Africa.	Client reference letter	
MR-S05	Complete bill of materials of licences and hardware with SKUs plus implementation services without pricing.	Compiled BOM with SKUs and no prices (Form TP-IT-9). Assessed at technical evaluation only	
MR-S06	KPC data and custom code stay in Kenya unless KPC approves otherwise in writing; every cloud service offered is declared with its hosting region.	Residency declaration and service-by-region table	
MR-S07	KPC receives the source code of, and the right to modify, every custom extension and partner add-on configuration delivered.	Signed IP undertaking	
MR-S08	Named key personnel, with CVs, ERP and MSOOS certifications, signed availability and a minimum time commitment per role.	CVs, certificates, signed commitment forms	

MR-S09	Named products and versions for every layer in the bill of materials template.	Completed BOM; no blank lines	
MR-S10	One resilience target across all documents: RPO ≤ 30 minutes, RTO ≤ 2 hours.	Signed compliance statement; DR design	
MR-S11	Hardware for the ERP database platform is listed in the ERP OEM's certified hardware directory and sizing uses the OEM's sizing tool on the volumetrics in section 2.2.6.2.	Directory references/links; sizing tool output	
MR-S12	The proposed MSOOS/TMS has at least two (2) production installations at liquid-petroleum pipeline or terminal operators, and a documented interface to the proposed ERP.	Reference letters; interface specification	
MR-S13	Kenyan statutory payroll (PAYE, SHIF, NSSF, Affordable Housing Levy) supported in the offered HCM.	Localisation statement and a reference site in Kenya	
MR-S14	KRA systems integration (iCMS , eTIMS etc) carried over or rebuilt, with no loss of current function.	Integration plan naming each interface	
MR-S15	Compliance with the Data Protection Act, 2019.	Data processing terms; registration with the ODPC where required	
MR-S16	A product roadmap commitment from the ERP OEM for the proposed ERP release and, for the MSOOS/TMS, from its OEM, each covering 10 years.	OEM letters	
MR-S17	Data migration from SAP ECC 6.0 is in scope, including historical hydrocarbon stocks and movement data for the period KPC specifies.	Migration scope statement; no exclusion of migration programs	
MR-S18	Complete integration inventory, listing every internal integration point between proposed components and every KPC-prescribed external interface.	Complete integration inventory	

Lead Bidder Requirements (MR-L01 to MR-L04)

MR-L01 to MR-L04 apply to the sole tenderer or, in a consortium, to the lead bidder alone, without aggregation of affiliates or members. The evidence is spelled out in full; incomplete years or bank letters without a balance or facility fail.

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-L01	Sound financial capacity: audited financial statements of the lead bidder for each of the last three (3) financial years. The firm shall be profitable in the last three financial years.	Signed audited statements for all three years, each with the auditor's opinion	

MR-L02	Lead bidder average annual turnover of at least USD 10 million over the last three (3) financial years.	Signed audited statements for all three years	
MR-L03	Positive net worth of the lead bidder in each of the last three (3) financial years.	Signed audited statements for all three years	
MR-L04	Bank reference letter dated within six (6) months of the closing date, stating account standing and either a balance range or a credit facility, and quoting the tender reference.	Original letter on the bank's letterhead, signed by an authorised officer, addressed to the Managing Director/CEO, KPC PLC, with the content set by account number, type and opening date; credit; duration of the relationship; bank officer's signature and seal	

OEM Financial Standing – ERP and MSOOS/TMS

MR-O01 to MR-O02 apply to the OEM of the offered ERP and to the OEM of the offered MSOOS/TMS.

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-O01	Sound financial capacity of the proposed ERP OEM and the MSOOS/TMS OEM. The firm shall be profitable, positive equity and an average revenue of at least USD 1 billion in the last three financial years.	To be confirmed by KPC from publicly available information from a reputable source	
MR-O02	The proposed MSOOS solution should be mature.	OEM statement on first release date.	

Technical Compliance – Software and Hardware

Software – ERP and MSOOS

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-T01	ERP and MSOOS release no older than one release behind the latest generally available release at contract signature.	Product schedule	
MR-T02	Hydrocarbon quantity conversion: ambient-to-standard volume and mass conversion using the API MPMS Chapter 11.1 / ASTM D1250 tables KPC applies, at 20°C reference, with density and temperature taken from measurement data; stock held in all stock keeping units KPC reports	Configuration statement naming tables and units;	
MR-T03	Hydrocarbon stock categories: Kenyan excise duty, bonded and duty-paid stock status, re-export and transit, financed and	Design statement per stock categories/status	

	un-financed stocks, quality, blocked, restricted stocks.		
MR-T04	Commercial custody functions: book transfers between customers, throughput and storage charges, ageing charges, and stock holds for collateral financing.	Design statement	
MR-T05	Gain/loss and stock reconciliation: pipeline and tank gain/loss calculated and allocated to customers under KPC's rules; daily book-to-physical reconciliation by product and location.	Allocation design.	
MR-T06	Asset management, including linear assets for pipeline sections, maintenance notifications from SCADA and condition data, inspection and integrity plans, and work clearance (permit to work).	Design statement	
MR-T07	Finance: IFRS reporting including IFRS 15 and IFRS 16, KES and USD multi-currency, Kenyan tax configuration, and reporting for a listed company.	Design statement	
MR-T08	Integration platform: a single integration platform for all interfaces, using only OEM-released APIs into the proposed ERP, with central interface monitoring and alerting.	Integration architecture	
MR-T09	Supportability: every software component within its OEM's mainstream maintenance for the contract term; ERP support contract; application lifecycle tooling for monitoring, testing and change control.	Maintenance dates per component; support contract terms	

Industry Add-ons and MSOOS/TMS

These apply to any industry add-on running on the ERP platform and to any separate MSOOS/TMS product.

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-A01	Certification: any add-on that runs on the ERP technology platform holds a current OEM certification for the offered release; any separate MSOOS/TMS product holds OEM-certified integration with the platform, or its interfaces use only OEM-released APIs.	Certificate reference from the OEM's certified solutions directory, or API list	
MR-A02	OT boundary: plant and SCADA data reach the ERP and MSOOS/TMS only through an OT DMZ designed to IEC 62443 zones and conduits; no direct connection from business systems to control networks.	OT integration architecture	

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-A03	Product support: 24×7 support for operationally critical functions (scheduling, loading, tickets) with response times stated, support cover in EAT time zone.	Standard OEM SLA	

Control Environment (MR-C01 to MR-C08)

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-C01	Access governance: a segregation-of-duties rule set covering KPC's processes, including hydrocarbon stock adjustments, and gain/loss postings; access requests through an approval workflow; quarterly access reviews	SoD rule set documentation; workflow design;	
MR-C02	Emergency and privileged access: Emergency IDs that are time-limited, logged and reviewed; no administrator profiles in production.	Emergency-access procedure;	
MR-C03	Change control: separate development, quality and production systems; all changes through approved transports with documented testing; production clients locked against direct change.	Configuration management procedure	
MR-C04	Audit logging: security audit log active, change documents on master data, table logging on critical tables, read-access logging for personal data, all forwarded to KPC's SIEM.	Logging design; SIEM integration	
MR-C05	Internal controls: a control library for ERP processes mapped to KPC's internal control framework, with automated monitoring of key controls, including dual approval and value limits on stock adjustments and gain/loss postings.	Control library; monitoring design	
MR-C06	Security baseline: secure-configuration baseline applied, OEM security notes applied monthly, vulnerability scanning of the solution stack, and code scanning of all custom code before transport.	Baseline document; patching procedure;	
MR-C07	Data protection: blocking and deletion of personal data at end of purpose, aligned with the Data Protection Act, 2019, and the data residency.	Information lifecycle design	
MR-C08	Hydrocarbon audit trail: stock movement traceable from meter or gauge ticket to general ledger posting; no manual stock override without recorded approval.	Audit-trail design;	

Hardware and Infrastructure (MR-H01 to MR-H10)

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-H01	Hardware listed in the OEM's certified and supported hardware directory (appliance or tailored data-centre integration); memory sized from the OEM sizing tool on the section 2.2.6.2 volumes plus five-year growth.	Directory references; sizing tool output; sizing workbook	
MR-H02	System landscape per site (primary and Disaster recovery): at minimum production, quality, development, sandbox and training systems, with the sizing of each stated.	Landscape diagram and sizing per system	
MR-H03	Operating system and virtualisation certified by the ERP OEM for the offered platform; any hypervisor used for production certified by the OEM for that use.	OS and hypervisor versions with OEM support references	
MR-H04	High availability: database system replication within the primary data centre with automated failover on certified cluster software; redundant application servers.	HA design; failover test plan	
MR-H05	Disaster recovery: replication to a DR site in Kenya meeting (RPO ≤ 30 min, RTO ≤ 2 h).	DR design; test plan	
MR-H06	Storage and backup: storage meeting the solution performance KPIs; backup through an OEM-certified backup interface; an immutable backup copy.	Storage KPI evidence; backup design	
MR-H07	Site and OT-edge equipment e.g. RFID readers, ATEX Mobile Tablets at depots and stations: industrial-rated, with hazardous-area certification where installed in classified areas.	Datasheets and certificates per item	
MR-H08	Lifecycle and support: every item supported by its OEM for at least five (5) years from go-live with 24×7, 4-hour response time for servers and storage; no item at end of life; exact models and part numbers in the BOM.	OEM end-of-life statements; support contract terms	
MR-H09	Management and monitoring: out-of-band management on a segregated network, signed firmware, and hardware alerts integrated with KPC's monitoring.	Management design	
MR-H10	OEM authorisation for the proposed infrastructure	OEM Authorization letter	

Delivery Experience

Ref	Mandatory Requirement	Evidence Required	Pass/Fail
MR-E01	MSOOS functional depth: across three projects, the bidder must have implemented at least three of these downstream functions: stock management, nominations, order fulfilment, shipment planning and loading operations.	Client letters naming the functions live and the go-live date	
MR-E02	ERP delivery at scale: at least two (2) ERP implementations or conversions brought to go-live by the tenderer in the last seven (7) years, each with at least 1,200 named users.	Client letters stating release, scope, users and go-live date	
MR-E03	Field integration: at least four (4) cited projects where tickets or measurements from terminal automation, SCADA, tank gauging or flow computers post automatically into the MSOOS.	Client letter; interface description	
MR-E04	Post-go-live support: at least one cited client supported by the tenderer for twelve (12) months or more after go-live.	Support contract extract or client letter	

D. STAGE 3 — TECHNICAL SCORING

Tenders passing Stages 1 and 2 shall be scored by each Evaluation Committee member independently. Final technical scores shall be the arithmetic mean of all members' scores. The minimum qualifying technical score is stated in the Data Sheet.

Technical Evaluation Lot 1: Provision of Programme Management Office (PMO) Services

Technical Evaluation Summary

No.	Evaluation Criterion	Points
1	Understanding of the Assignment and PMO Methodology	20
2	Programme Governance, Controls and Reporting	15
3	Programme Planning, Scheduling and Resource Management	15
4	Risk, Issue, Change and Quality Management	15
5	Benefits Realization and Stakeholder Management	10
6	Relevant PMO and Transformation Experience	10
7	Qualifications and Experience of Key Personnel	10
8	Knowledge Transfer, Local Participation and Sustainability	5
	Total	**100**

Minimum Technical Score: 75 Marks

Understanding of the Assignment and PMO Methodology – 20 Marks

Submit FORM TP-IT-5: IMPLEMENTATION OF METHODOLOGY AND PROJECT PLAN

Ref	Sub-Criterion	Points	Scoring Guidance
PM1.1	Understanding of KPC's business objectives and programme requirements	6	Comprehensive understanding = 6; Good understanding = 4; Limited understanding = 2; Poor/None = 0

PM1.2	Proposed PMO methodology and work plan	6	Comprehensive methodology aligned to requirements = 6; Good = 4; Adequate = 2; Poor = 0
PM1.3	PMO mobilization and transition approach	4	Comprehensive and practical = 4; Adequate = 2; Poor/None = 0
PM1.4	Alignment of PMO approach with KPC governance structures	4	Comprehensive alignment = 4; Adequate = 2; Poor/None = 0
	Total	**20**	

Programme Governance, Controls and Reporting – 15 Marks
Submit FORM TP-IT-5: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN

Ref	Sub-Criterion	Points	Scoring Guidance
PM2.1	Programme governance framework and decision-making structure	4	Comprehensive framework with clear roles, authorities and escalation mechanisms = 4; Good = 3; Adequate = 2; Poor/None = 0
PM2.2	Programme reporting and management dashboards	3	Comprehensive reporting framework with relevant KPIs and dashboards = 3; Adequate = 2; Poor/None = 0
PM2.3	Programme controls and assurance mechanisms	3	Comprehensive controls and assurance framework = 3; Adequate = 2; Poor/None = 0
PM2.4	Programme documentation and records management	2	Comprehensive = 2; Adequate = 1; Poor/None = 0
PM2.5	Steering Committee and executive reporting support	3	Comprehensive decision-support approach = 3; Adequate = 2; Poor/None = 0
	Total	**15**	

Programme Planning, Scheduling and Resource Management – 15 Marks
Submit FORM TP-IT-5: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN

Ref	Sub-Criterion	Points	Scoring Guidance
PM3.1	Integrated programme planning and scheduling	4	Comprehensive methodology with integrated master schedule = 4; Good = 3; Adequate = 2; Poor/None = 0
PM3.2	Dependency and inter-workstream management	3	Comprehensive dependency management approach = 3; Adequate = 2; Poor/None = 0
PM3.3	Resource planning and utilization management	3	Comprehensive resource planning and capacity management = 3; Adequate = 2; Poor/None = 0
PM3.4	Milestone and critical-path management	3	Comprehensive milestone and critical-path controls = 3; Adequate = 2; Poor/None = 0
PM3.5	Programme performance tracking and early-warning mechanisms	2	Comprehensive = 2; Adequate = 1; Poor/None = 0
	Total	**15**	

Risk, Issue, Change and Quality Management – 15 Marks

Ref	Sub-Criterion	Points	Scoring Guidance

PM4.1	Programme risk management framework	4	Comprehensive identification, assessment, mitigation and monitoring = 4; Good = 3; Adequate = 2; Poor/None = 0
PM4.2	Issue and escalation management	3	Comprehensive issue management and escalation process = 3; Adequate = 2; Poor/None = 0
PM4.3	Change and scope management	3	Comprehensive change control and scope management = 3; Adequate = 2; Poor/None = 0
PM4.4	Quality assurance and quality control	3	Comprehensive QA/QC framework = 3; Adequate = 2; Poor/None = 0
PM4.5	Programme risk and issue reporting	2	Comprehensive reporting and monitoring = 2; Adequate = 1; Poor/None = 0
	Total	**15**	

Benefits Realization and Stakeholder Management – 10 Marks

Ref	Sub-Criterion	Points	Scoring Guidance
PM5.1	Benefits realization framework and tracking	3	Comprehensive framework with measurable benefits = 3; Adequate = 2; Poor/None = 0
PM5.2	KPI and programme performance management	2	Comprehensive KPI framework = 2; Adequate = 1; Poor/None = 0
PM5.3	Stakeholder engagement and communication	3	Comprehensive stakeholder engagement and communication approach = 3; Adequate = 2; Poor/None = 0
PM5.4	Business-user and executive engagement	2	Comprehensive approach = 2; Adequate = 1; Poor/None = 0
	Total	**10**	

Relevant PMO and Transformation Experience – 10 Marks

Submitted In the format provided in FORM TP-IT-2: TENDERER PROFILE AND CORPORATE CREDENTIALS

Relevant IT project experience)

Ref	Sub-Criterion	Points	Scoring Guidance
PM6.1	Comparable PMO assignments	4	5 or more comparable assignments = 4; 4 = 3; 3 = 2; 2 = 1; Less than 2 = 0
PM6.2	Enterprise ICT / Digital Transformation programmes	3	4 or more comparable programmes = 3; 3 = 2; 2 = 1; Less than 2 = 0
PM6.3	ERP / enterprise systems transformation programmes	2	3 or more comparable programmes = 2; 2 = 1; Less than 2 = 0
PM6.4	Multi-vendor programme management expérience	1	2 or more comparable programmes = 1; Less than 2 = 0
	Total	**10**	

Qualifications and Experience of Key Personnel – 10 Marks

Submit FORM TP-IT-6: PROPOSED TEAM — KEY PERSONNEL

Ref	Sub-Criterion	Points	Scoring Guidance
PM7.1	Programme Director	3	≥15 years relevant experience = 3; 10–14 years = 2; 7–9 years = 1; <7 years = 0
PM7.2	Programme Manager / PMO Lead	2	≥10 years relevant experience = 2; 7–9 years = 1; <7 years = 0
PM7.3	Planning and Controls Lead	1	≥8 years relevant experience = 1; <8 years = 0

PM7.4	Risk / Quality Lead	1	≥8 years relevant experience = 1; <8 years = 0
PM7.5	Change Management Lead	1	≥8 years relevant experience = 1; <8 years = 0
PM7.6	Business / Transformation Lead	1	≥8 years relevant experience = 1; <8 years = 0
PM7.7	Other Relevant Specialists	1	Strong multidisciplinary team with relevant qualifications = 1; otherwise = 0
	Total	**10**	

Knowledge Transfer, Local Participation and Sustainability – 5 Marks

Submit FORM TP-IT-5: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN

Ref	Sub-Criterion	Points	Scoring Guidance
PM8.1	Knowledge transfer to KPC resources	2	Comprehensive structured programme = 2; Adequate = 1; Poor/None = 0
PM8.2	Local participation	1	Strong local participation = 1; Limited/None = 0
PM8.3	PMO capability transfer and sustainability	1	Comprehensive capability transfer = 1; Limited/None = 0
PM8.4	Exit and transition approach	1	Comprehensive transition approach = 1; Limited/None = 0
	Total	**5**	

Technical Evaluation – Lot 2: Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution

Stage 3A – Technical Proposal Evaluation (100 Marks)

Only Lot 2 tenders that pass Stages 1 and 2 are scored. Stage 3A carries 100 marks; the pass mark to progress to Stage 3B demonstration is 75%.

No.	Evaluation Criterion	Points
DT1	Solution scope and fit to KPC business requirements	11
DT2	Architecture and integration	9
DT3	Data Migration from SAP ECC 6.0 experience, infrastructure and DR	11
DT4	Cybersecurity, identity and data protection	9
DT5	Implementation methodology	19
DT6	Solution provider experience	11
DT7	Key Personnel	20
DT8	Architecture coherence and minimal disruption	10
	Total Stage 3A	100

DT1 Solution scope and fit-to-KPC business requirements – 11 Marks

Submit FORM TP-IT-3: TECHNICAL SOLUTION DESCRIPTION, FORM TP-IT-4 TECHNICAL COMPLIANCE MATRIX

Ref	Sub-Criterion	Points	Scoring Guidance
DT1.1	Fit-to-KPC business requirements	6	Share of the requirements in section 2.2.4 met by standard, released functionality of the offered release, each mapped to product documentation. Highest marks where gaps are few, named and closed by configuration rather than development.
DT1.2	Oil and gas design	4	Design for KPC's pipeline, depot and terminal processes: quantity conversion, owner entitlement, ASE exchanges, hydrocarbon stock categories, CFA, scheduling and terminal operations.
DT1.3	e-procurement and HCM fit	1	Coverage of source-to-pay including supplier portal and HCM/payroll requirements functionality.

DT2 Architecture and integration – 9 Marks

Submit FORM TP-IT-3

Ref	Sub-Criterion	Points	Scoring Guidance
DT2.1	Extensibility	5	Ease of extending functionality and support for extensions development lifecycle.
DT2.2	External integration	2	KRA iCMS/eTIMS, banks, SCADA/ATG and other external interfaces on the single integration platform, using released APIs, with monitoring and error handling.
DT2.3	Analytics hosting	2	Analytics architecture, hosting and data residency compliant with Data Protection Act; clear data flows and minimal data copying.

DT3 SAP ECC 6.0 Data Migration experience, infrastructure and DR – 11 Marks

Submit FORM TP-IT-3, FORM TP-IT-2A and client-confirmed conversion references

Ref	Sub-Criterion	Points	Scoring Guidance
DT3.1	SAP ECC 6.0 and data conversion experience to the new platform	3	scores the quality of the tenderer's data conversion record on the SAP ECC 6.0 conversions
DT3.2	High availability on certified hardware	5	HA design on OEM-certified hardware and cluster software, with a failover test plan.
DT3.3	Disaster recovery	3	DR design meeting RPO ≤ 30 minutes and RTO ≤ 2 hours at a Kenyan DR site, with test approach and evidence of achievability.

DT4 Cybersecurity, identity and data protection – 9 Marks

Submit FORM TP-IT-3 and FORM TP-IT-8

Ref	**Sub-Criterion**	**Points**	**Scoring Guidance**
DT4.1	Authorisations and SoD	4	Role design, SoD rule set and access governance.
DT4.2	Identity and SSO	3	Integration design with KPC's IAM and PAM platforms, SSO and MFA across all components.
DT4.3	Patching, SIEM and data protection	2	Security patching cadence, SIEM log forwarding and personal-data controls.

DT5 Implementation methodology – 19 Marks

Submit FORM TP-IT-5B: IMPLEMENTATION METHODOLOGY AND PROJECT PLAN

Ref	**Sub-Criterion**	**Points**	**Scoring Guidance**
DT5.1	OEM methodology tailoring	2	The OEM's implementation methodology tailored to KPC's releases, sites and conversion, not a generic description.
DT5.2	Plan realism	3	Resource-loaded plan within 18 months to go-live, with dependencies, KPC inputs and critical path shown and achievable.
DT5.3	Governance and QA	2	Governance framework proposed, quality gates and stage-gate evidence.
DT5.4	Knowledge transfer	4	Training, knowledge transfer and change plan for KPC's user groups and sites with measurable exit criteria.
DT5.5	Transition approach	6	Ease of transition to the proposed solution (organizational & Technical), with downtime, fallback and parallel-run arrangements.
DT5.6	Testing	2	Test strategy covering unit, SIT, performance, security, DR and UAT, with tooling and entry/exit criteria.

DT6 Solution Provider Experience – 11 Marks

Submit FORM TP-IT-2A: TENDERER PROFILE AND CORPORATE CREDENTIALS

Ref	**Sub-Criterion**	**Points**	**Scoring Guidance**

DT6.1	Successful ERP projects	3	Number and **relevance** of completed ERP projects.
DT6.2	Successful MSOOS projects	3	Number and **relevance** of completed MSOOS projects, at operators with a similar operating model.
DT6.3	ECC IS-Oil conversions and Africa	3	Number of completed SAP ECC 6.0 IS-Oil conversions projects.
DT6.4	Experience integrating ERP with third-party enterprise applications, operational technology and external systems	2	Number of completed projects involving integrations

DT7 Key personnel – 20 Marks

Submit FORM TP-IT-6: PROPOSED TEAM — KEY PERSONNEL and commitment forms

Ref	Sub-Criterion	Points	Scoring Guidance
DT7.1	Project Manager	2	meets the qualification and experience requirement with at least two comparable programmes in the role and signed commitment
DT7.2	Solution Architect	3	meets the qualification and experience requirements, with current OEM architecture certification.
DT7.3	Functional Lead(s)	3	meets the qualification and experience requirements, with current ERP functional certification
DT7.4	MSOOS Functional Lead	3	meets the qualification and experience requirements, with current MSOOS oil and gas downstream experience.
DT7.5	Technical Lead	2	meets the qualification and experience requirements, with current ERP Technical certification
DT7.6	Integration Lead	1	meets the qualification and experience requirements, with current ERP integration platform certification
DT7.7	Data Migration Lead	2	meets the qualification and experience requirements with SAP ECC 6.0 conversion experience.
DT7.8	Security Lead	1	meets the qualification and experience requirements with recognised security certification.
DT7.9	Change Management Lead	1	meets the qualification and experience requirements with recognised change-management certification.
DT7.10	Development Lead	2	meets the qualification and experience requirements, with current ERP development certification

DT8 Architecture coherence and minimal disruption – 10 Marks

Submit FORM TP-IT-3

Ref	Sub-Criterion	Points	Scoring Guidance

DT8.1	Same Technology stack for ERP and MSOOS	3	ERP and MSOOS on one platform and data model or at a minimum separate product integrated through OEM-certified integration or released APIs with shared master data.
DT8.2	Internal integration points	3	Fewer internal integration point/distinct interface between separately deployed components offered by the tenderer
DT8.3	Single source of truth	2	Shows one system of record for ERP, MSOOS & TMS, with no dual mastering.
DT8.4	Business continuity	2	Shows the lowest credible maximum planned downtime per site, with fallback and continuity of loading and billing.

E. STAGE 3B — SCRIPTED DEMONSTRATION (LOT 2, PASS/FAIL)

Each script is pass/fail; a tenderer must pass every script to proceed to financial evaluation. The demonstration is not scored and does not add marks.

i. Data set: KPC issues a sample data set, the worked examples and the tolerances to all invited tenderers at the same time, at least 3 days before the first session.

ii. Offered release, live: demonstrations use the offered release, operated live by the tenderer. Slides, recordings, screenshots or another client's system are not accepted.

iii. Pass/fail: each script is assessed pass or fail by the Evaluation Committee against the "pass when" condition, with reasons recorded. Failing any script ends the evaluation of that tender.

iv. Conduct: sessions are held online.

v. OT and regulatory simulators: Bidders may use their own simulators or test environments.

Script	What must be shown	Pass when	Pass/Fail
DEMO-01	Pipeline transfer between terminals, using AGO and MSP; in the process demonstrate issuing and receiving to/from a tank; ambient-to-standard conversion, transmix/interface and any movement variance	Quantities movements and conversion are recorded accurately.	
DEMO-02	Demonstrate role-based access control (RBAC). Access is granted to users only through roles, and each role's permissions can be restricted at three levels: business object, field, and table/data.	Two test users with different roles attempt the same tasks. One is permitted and the other is denied at each level below, and the denials are shown to be enforced by the system, not by the screen layout. Generate segregation-of-duties conflict report and an audit-trail query	
DEMO-03	Asset management: a SCADA/DCS alarm or condition reading creates a	End-to-end flow without manual re-keying	

Script	What must be shown	Pass when	Pass/Fail
	maintenance notification and work order, through to cost settlement.		

Lot 2 Combined Technical Score

The Lot 2 technical score is the Stage 3A score out of 100 marks. A Lot 2 tenderer qualifies for financial evaluation only if it scores at least 75 marks at Stage 3A and passes all 3 Stage 3B demonstration scripts.

F. STAGE 5 — FINANCIAL AND TCO EVALUATION

Only tenderers that meet the minimum technical requirement (Lot 1: 75 marks; Lot 2: at least 75 of 100 marks at Stage 3A and a pass in every Stage 3B script) shall have their Financial Proposals evaluated.

For Lot 2, In the financial evaluation, the priced licence and hardware BOM shall be compared to the non-priced BOM submitted as part of technical bid for completeness.

F.1 Financial Proposal Completeness Review

- All items in the Technical Proposal are priced in the BOM;
- All cost components for LOT 1 & 2 are separately identified;
- Arithmetic errors are corrected (unit prices prevail over totals; words prevail over figures);
- Currency conversion applied at rates specified in the Data Sheet;
- Unpriced items shall be treated as follows:

  The adjustment shall be based on the highest price of the item or component as quoted in other substantially responsive Tenders. If the price of the item or component cannot be derived from the price of other substantially responsive Tenders, the Procuring Entity shall use its best estimate.

F.2 Total Cost of Ownership (TCO) Calculation – LOT 2 Only

KPC PLC evaluates IT tenders on TCO basis, not lowest initial price. The evaluated cost for financial scoring shall be the TCO over the period stated in the Data Sheet.

The TCO shall include:

LOT 2 - TOTAL COST OF OWNERSHIP —

Category	Year 1 (USD)	Year 2 (USD)	Year 3 (USD)	Year 4 (USD)	Year 5 (USD)	Year 6 (USD)	Total Cost (USD)
Software / Subscriptions							
OEM Support							
Application Support							
Infrastructure Support							
Cloud / Hosting							

Implementation (One-off)							
Other Recurring Costs							
TOTAL RECURRING COST	—	—	—	—	—	—	—

Assumption while calculating 6-year TCO

i. The award and contract term shall be for three years renewable once at the **same price**. No rate change shall be allowed in the first six (6) years of contract.
ii. Subscription and support pricing shall be **fixed for the initial term of six (6) years from first Production Go-Live.**
iii. Ever green environment for the 6 years
iv. Tenderer has disclosed all the cost associated with the delivery of the entire scope.
v. There will be no material hardware changes within the six (6) years.

F.3 Financial Scoring

The Tenderer with the lowest evaluated TCO shall receive the maximum financial score of 100 points. Others shall be scored as:

Financial Score = (Lowest TCO / Tenderer's TCO) × 100

For Lot 2, the financial score is out of 20 marks: Lot 2 Financial Marks = 20 × (Lowest TCO / Tenderer's TCO).

G. COMBINED SCORING AND AWARD RECOMMENDATION

Combined Score = (Technical Score × Technical Weight%) + (Financial Score × Financial Weight%)

The Tenderer with the highest Combined Score shall be recommended for contract award, subject to post-qualification verification.

Final Evaluation – Award Criteria

The Financial Score shall be determined out of 100 **Marks**.
For **Lot 1**, the principal price comparison shall be based on the **Total Evaluated PMO Cost**.

For **Lot 2**, the principal price comparison shall be based on the **six-year Total Cost of Ownership (TCO)**.

The financial evaluation shall consider all costs required for complete delivery of the respective Lot in accordance with the Tender Document.

Quality and Cost Based Selection (QCBS)

The Final Evaluation Score shall be calculated using the following weighting:

Evaluation Component	**Weight**
Technical Evaluation	**Lot 1: 80%; Lot 2: 80%;**
Financial Evaluation	**Lot 1: 20%; Lot 2: 20%;**

Total	**Lot 1: 100%; Lot 2: 100 marks**

The Final Evaluation Score shall be calculated as:

Lot 1: Final Score = (Technical Score × 80%) + (Financial Score × 20%)
Lot 2: Final Score = (Technical Score × 80%) + (Financial Score × 20%)

The Tenderer achieving the highest Final Evaluation Score shall be ranked first and awarded.
A Tenderer can only be awarded one lot

H. POST-QUALIFICATION VERIFICATION

Before issuing the Letter of Award, KPC PLC shall verify:

Tax Compliance	Valid KRA Tax Compliance Certificate for Kenyan firms.
OEM Authorisations	i. All OEM Authorisation Letters current and verified with OEMs. ii. A 10 year Product Roadmap signed commitment from the OEM
Financial Standing	i. Audited accounts for last 3 years- LOT 1- Minimum USD 1 million turn over the last 3 years. LOT 2 - Minimum USD 10 million turn over the last 3 years. ii. Financial Stability: The Tenderer shall have maintained a positive net worth during the last 3 years. iii. Bank reference letter issued in the last 6 months to demonstrate access to sufficient financial resources.
Client References	• Minimum 2 satisfactory references from similar IT projects —LOT 1- Similar project management programmes • LOT 2- Similar Digital transformation projects KPC PLC may contact referees
Key Personnel Availability	All Key Personnel confirmed available for this project
No Adverse Findings	Not debarred; no recent corruption conviction; no material adverse litigation

KENYA PIPELINE COMPANY PLC

CONTRACT FOR THE DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION

General Conditions of Contract, Special Conditions of Contract and SLA Schedule)

PART 4 – GENERAL CONDITIONS OF CONTRACT

SECTION V: GENERAL CONDITIONS OF CONTRACT FOR IT PROCUREMENT (GCC-IT)

These General Conditions apply to all IT contracts entered into by KPC PLC, covering hardware, software, licences, implementation services, support, managed services or any combination. The SCC (Section VI) supplements and amends the GCC-IT for each specific contract.

1. DEFINITIONS

In addition to the definitions in ITT Clause 2, in this Contract:

a) "Acceptance" means KPC PLC's written confirmation (Form C3) that a Deliverable meets the Acceptance Criteria;

b) "Acceptance Criteria" means the technical, functional and performance standards against which Deliverables are assessed;

c) "Affiliate" means any entity controlling, controlled by or under common control with a Party;

d) "Bug" means a defect causing the system to fail to operate in accordance with its specification;

e) "Change Request" means a written instruction from KPC PLC to change the scope of the Works;

f) "Contract" means the legal agreement comprising the Contract Agreement, SCC, GCC-IT, Technical Specifications/Terms of Reference, BOM, SLA Schedule and all Appendices;

g) "Data" means all information, content and materials owned by or entrusted to KPC PLC that the Vendor accesses under this Contract;

h) "End of Life (EoL)" means the date after which the OEM no longer provides security patches, updates or technical support;

i) "Escrow Agent" means the independent third party holding the Escrow Materials;

j) "Escrow Materials" means the source code, build tools, documentation and other materials deposited in escrow;

k) "Go-Live Date" means the date on which the system becomes operational and Acceptance is issued;

l) "Hardware" means physical IT equipment supplied under this Contract;

m) "Hypercare Period" means the intensive post-Go-Live support period as specified in the SCC;

n) "Incident" means an unplanned interruption to or degradation of IT services;

o) "Intellectual Property Rights" means patents, copyright, database rights, trade secrets, trademarks, know-how and similar rights;

p) "Licence" means the right granted to KPC PLC to use Software under defined terms;

q) "Managed Service" means the ongoing operational management of IT systems by the Vendor under the SLA;

r) "MTTR" means Mean Time to Repair — the average time taken to restore a failed system;

s) "Personal Data" has the meaning given in the Data Protection Act 2019 of Kenya;

t) "RTO" means Recovery Time Objective — the maximum acceptable time to restore IT services after a disruption;

u) "RPO" means Recovery Point Objective — the maximum acceptable data loss in the event of a disruption;

v) "SLA" means the Service Level Agreement in Schedule A of the SCC;

w) "Software" means computer programs, applications, firmware and associated materials supplied under this Contract;

x) "Upgrade" means a new version of Software containing significant new functionality;

y) "Update" means a release of Software containing bug fixes, security patches or minor enhancements;

z) "Vendor" means the successful Tenderer awarded this Contract;

2. APPLICABLE LAW AND JURISDICTION

2.1 This Contract shall be governed by the applicable laws of Kenya.

2.2 The Parties submit to the exclusive jurisdiction of the courts of Kenya, subject to the dispute resolution provisions in GCC Clause 27.

2.3 The validity, formation and effect of electronic contracts, digital signatures and electronic records under this Contract shall be governed by the Kenya Information and Communications (Electronic Transactions) Regulations.

3. CONTRACT DOCUMENTS AND PRIORITY

3.1 In the event of conflict, the Contract Documents shall prevail in this order: (a) Contract Agreement; (b) Special Conditions of Contract; (c) Detailed special conditions of contract (d) Technical Specifications/Terms of Reference; (e) Change Requests and formal amendments; (f) SLA Schedule; (g) General Conditions of Contract (this Section); (h) Bill of Materials; (i) the Vendor's Technical Proposal.

4. SCOPE OF SUPPLY AND SERVICES

4.1 The Vendor shall supply, deliver, install, configure, test, commission and hand over the IT system as specified in the Technical Specifications/Terms of Reference, BOM and Contract. Unless expressly excluded in the SCC, the Vendor's obligations include:

(a) Supply of all hardware, software and licences stated in the BOM;

(b) Physical delivery to KPC PLC's designated site(s);

(c) Hardware installation, rack-mounting, cabling and commissioning;

(d) Software installation, configuration and customisation;

(e) Integration with KPC PLC's specified existing systems;

(f) Data migration as specified in the Technical Specifications/Terms of Reference;

(g) Testing — unit, integration, system, UAT and performance;

(h) Training of KPC PLC's personnel and administrators;

(i) Documentation — technical, operational and user manuals;

(j) Go-Live support and Hypercare;

(k) Project management throughout;

(l) Ongoing support and maintenance under the SLA.

4.2 The Vendor shall not subcontract the core delivery obligations without KPC PLC's prior written approval. Approved subcontractors shall be identified in the Contract. The Vendor remains fully responsible for all subcontracted activities.

5. HARDWARE SUPPLY

5.1 All hardware shall be: new and unused; of the most current commercially available model unless otherwise specified; free from defects in materials and workmanship; and not End-of-Life at the time of delivery or for a period of at least 5 years after delivery.

5.2 The Vendor warrants that all hardware is genuine, sourced through authorised channels, not counterfeit, and is eligible for OEM warranty and support.

5.3 Hardware shall be delivered to KPC PLC's designated site(s) with: itemised delivery notes; packing lists; OEM serial numbers for all serialised items; and all manuals, accessories and cables.

5.4 KPC PLC shall conduct incoming inspection. If hardware is found defective or non-conforming at inspection or within the Warranty Period, the Vendor shall replace it at no cost to KPC PLC within the period stated in the SCC.

6. SOFTWARE AND LICENCES

6.1 The Vendor warrants that all software is: licensed for use by KPC PLC under the terms set out in the Contract; genuine and sourced from authorised channels; not subject to any third-party rights that would prevent KPC PLC's use as specified; and not at End-of-Life or End-of-Support at the time of delivery or for at least 3 years after Go-Live.

6.2 Licence Grant and Scope: The Vendor grants KPC PLC the right to use the software in accordance with the Licence terms stated in the BOM. Unless stated otherwise: (a) licences are perpetual (not time-limited); (b) licences are site-wide or user-based as specified in the BOM; (c) KPC PLC may make backup copies; (d) KPC PLC may engage third parties to operate the software on its behalf.

6.3 Open-Source Components: Where the proposed system incorporates open-source software, the Vendor shall: (a) provide a complete Software Bill of Materials (SBOM) listing all open-source components and their licences; (b) ensure all open-source licences are compatible with KPC PLC's use; (c) proactively monitor and patch open-source vulnerabilities.

6.4 SaaS and Cloud Services: Where the contract involves SaaS or cloud services: (a) the Vendor shall provide the SaaS service with the uptime and performance levels in the SLA; (b) KPC

PLC retains ownership of all data uploaded to or generated in the cloud service; (c) the Vendor shall provide a data export facility enabling KPC PLC to extract all data in a standard format at any time; (d) on termination, the Vendor shall provide all KPC PLC data in the agreed format within 30 days.

7. SOFTWARE ESCROW

7.1 Where specified in the SCC (mandatory for custom-developed software and critical bespoke systems), the Vendor shall, within 60 days of Go-Live, deposit Escrow Materials with an independent Escrow Agent approved by KPC PLC.

7.2 Escrow Materials shall include: complete, compilable source code; build tools and scripts; third-party component licences; technical documentation; and installation/deployment instructions sufficient for a competent third party to maintain the system.

7.3 The Vendor shall update the Escrow deposit within 30 days of any material change to the system.

7.4 Escrow Release Triggers: KPC PLC may access the Escrow Materials if: (a) the Vendor becomes insolvent or ceases to trade; (b) the Vendor fails to provide contracted support and does not remedy within 30 days of written notice; (c) the Vendor ceases to maintain the software or support the relevant version; or (d) any other trigger event agreed in the SCC.

7.5 On release, KPC PLC shall use the Escrow Materials only to maintain or operate the system and shall not use them for any other purpose or disclose them to third parties.

8. DELIVERY, INSTALLATION AND COMMISSIONING

8.1 The Vendor shall deliver, install and commission the system in accordance with the Implementation Plan. Time is of the essence and delays shall attract liquidated damages as specified in the SCC.

8.2 The Vendor shall conduct the following tests before requesting KPC PLC's acceptance: (a) Factory Acceptance Test (FAT) or internal testing, where applicable; (b) Site Acceptance Test (SAT) at KPC PLC's site; (c) System Integration Test (SIT) confirming compatibility with connected systems; (d) User Acceptance Test (UAT) with KPC PLC's end-users; (e) Performance/Load Test confirming system performance under expected and peak loads; (f) Security Test (penetration test or vulnerability scan) by KPC PLC or an independent party.

8.3 The Vendor shall provide KPC PLC with 5 working days' advance notice of any test requiring KPC PLC attendance.

9. ACCEPTANCE

9.1 KPC PLC shall issue a Provisional Acceptance Certificate (PAC) upon satisfactory completion of UAT, SIT and performance testing. The PAC marks the start of the Warranty Period and Hypercare Period.

9.2 KPC PLC shall issue a Final Acceptance Certificate (FAC) upon: (a) expiry of the Hypercare Period with no unresolved Critical or High bugs; (b) delivery of all documentation; (c) completion of all training; (d) completion of knowledge transfer; and (e) if applicable, successful Escrow deposit.

9.3 Neither acceptance nor payment releases the Vendor from warranty, support or other obligations.

9.4 Deemed Acceptance: If KPC PLC fails to review and respond to a submitted Deliverable within 45 working days, the Deliverable shall be deemed accepted.

10. PROJECT MANAGEMENT

10.1 The Vendor shall appoint a qualified Project Manager as named in the Contract. The Project Manager shall be the primary point of contact for all contract administration matters and shall attend weekly or bi-weekly project review meetings as agreed.

10.2 The Vendor shall provide: (a) weekly written project status reports during the implementation phase; (b) a risk register updated monthly; (c) updated project plan with actual vs planned progress; (d) escalation of issues promptly to KPC PLC's Project Sponsor.

10.3 KPC PLC shall designate a KPC PLC Project Manager who shall have authority to: give instructions within the agreed scope; approve or reject Deliverables; and escalate issues. KPC PLC's Project Manager shall not have authority to authorise changes to the Contract Price or scope without written Contract Amendment.

11. CHANGE MANAGEMENT

11.1 KPC PLC may at any time request changes to the scope of the Contract by submitting a Change Request in writing. The Vendor shall respond within 10 working days with: (a) impact on scope; (b) impact on Contract Price; (c) impact on timeline; and (d) any other material effects.

11.2 No change shall be implemented without a written Contract Amendment signed by both Parties specifying the agreed scope, price and timeline adjustments.

11.3 Where a change is required urgently (for example, a critical security patch or emergency capability), KPC PLC may instruct the Vendor to proceed immediately. The commercial impact shall be agreed within 21 days of the instruction.

12. WARRANTY

12.1 The Vendor warrants that during the Warranty Period stated in the SCC: (a) hardware is free from defects in materials and workmanship; (b) software operates materially in accordance with its specification; and (c) the system meets the performance standards in the Technical Specifications/Terms of Reference.

12.2 During the Warranty Period, the Vendor shall remedy any defect notified by KPC PLC within the response and resolution times specified in the SLA, at no additional cost to KPC PLC.

12.3 The Warranty Period shall be extended by any period during which the system or a significant component was unavailable due to a Vendor-caused defect.

13. SERVICE LEVEL AGREEMENT (SLA)

13.1 Following the Go-Live Date (or from the date specified in the SCC), the Vendor shall provide support, maintenance and managed services in accordance with the SLA Schedule (Section VI-A).

13.2 The Vendor shall maintain a local helpdesk in Kenya (or a dedicated support facility meeting KPC PLC's requirements) staffed during the operating hours stated in the SLA.

13.3 Incidents shall be classified and responded to in accordance with the priority levels and response/resolution times in the SLA Schedule.

13.4 Service Credits: Where the Vendor fails to meet SLA targets, KPC PLC shall be entitled to Service Credits as specified in the SLA Schedule. Service Credits are the primary remedy for SLA failures and do not exclude other remedies where failures are persistent or material.

13.5 SLA Reporting: The Vendor shall provide monthly SLA performance reports within 5 working days after month-end, showing: uptime achieved; incident volumes by priority; average response and resolution times; open incidents; and service credit calculations.

13.6 Annual SLA Review: The Parties shall review SLA targets annually and may agree adjustments by written Amendment.

14. CYBERSECURITY OBLIGATIONS

14.1 The Vendor shall maintain and implement a documented Information Security Management System (ISMS) aligned with ISO/IEC 27001 or equivalent throughout the Contract.

14.2 The Vendor shall: (a) conduct annual penetration testing of systems provided to KPC PLC by an independent accredited tester and provide results to KPC PLC within 30 days; (b) remediate Critical vulnerabilities within 48 hours of discovery; High vulnerabilities within 7 days; Medium within 30 days; (c) maintain a Software Bill of Materials (SBOM) for all software components and update it within 14 days of any change; (d) apply all vendor-released security patches within the timeframes in the SLA Schedule; (e) notify KPC PLC immediately (within 4 hours) of any security incident affecting KPC PLC's systems or data.

14.3 For cloud or managed services: (a) the Vendor shall maintain SOC 2 Type II certification or equivalent and provide current audit reports annually; (b) all data transmission shall be encrypted using TLS 1.2 or higher; (c) data at rest shall be encrypted using AES-256 or equivalent; (d) multi-factor authentication shall be enforced for all administrative access.

14.4 The Vendor shall not install any back-doors, remote access tools, or monitoring agents on KPC PLC's systems without prior written disclosure and approval.

14.5 Supply Chain Security: The Vendor shall disclose all third-party components and subcontractors who have access to KPC PLC's systems or data, and shall ensure they are subject to equivalent security obligations.

15. DATA PROTECTION

15.1 The Vendor shall comply with the Data Protection Act 2019 of Kenya in all processing of Personal Data under this Contract.

15.2 The Vendor processes Personal Data as a Data Processor acting on KPC PLC's documented instructions only. The Vendor shall: (a) process Personal Data only for purposes of this Contract; (b) implement appropriate technical and organisational security measures; (c) not engage sub-processors without KPC PLC's prior written approval; (d) assist KPC PLC in responding to data subject rights requests; (e) notify KPC PLC of any Personal Data breach within 24 hours of discovery; (f) not transfer Personal Data outside Kenya without KPC PLC's prior written consent and appropriate safeguards; (g) securely return or destroy all Personal Data at contract end.

15.3 Data Residency: Unless otherwise specified in the SCC, all KPC PLC data shall be stored and processed within Kenya.

15.4 Right to Audit: KPC PLC may conduct or commission data protection audits of the Vendor's systems and processes relating to KPC PLC's data. The Vendor shall cooperate fully.

16. INTELLECTUAL PROPERTY

16.1 Pre-Existing IP: Each Party retains ownership of its pre-existing intellectual property. The Vendor grants KPC PLC a licence to use the Vendor's pre-existing IP to the extent incorporated in the Deliverables or necessary to use them.

16.2 Custom Development: All software, code, configurations, databases, interfaces and other materials developed specifically for KPC PLC under this Contract (Custom Work) shall be the exclusive property of KPC PLC from creation. The Vendor assigns all such IP to KPC PLC. The Vendor shall execute any document required to perfect this assignment.

16.3 Shared Background IP: Where the Vendor incorporates its background IP in Custom Work, the Vendor grants KPC PLC a non-exclusive, irrevocable, royalty-free, perpetual licence to use it for the purpose of using the Custom Work.

16.4 OEM and Third-Party Software: The Vendor shall ensure that all OEM and third-party software licences are transferred or granted to KPC PLC in the Vendor's name or directly from the OEM/licensor as specified in the BOM.

16.5 IP Indemnity - Vendor: The Vendor shall indemnify KPC PLC against any claim that the Deliverables infringe a third party's intellectual property rights, provided the Deliverables are used as specified.

16.6 IP Indemnity - KPC PLC: KPC PLC shall indemnify the Vendor against claims arising from designs, specifications or materials provided by KPC PLC that cause infringement.

17. PAYMENT

17.1 KPC PLC shall pay the Vendor in accordance with the payment schedule in the SCC. Typical IT payment milestones for implementation projects include: Contract Signing; Hardware Delivery and Inspection; Software Installation; SIT/UAT Completion; Provisional Acceptance (PAC); Final Acceptance (FAC); End of Hypercare Period. Any payment that represents a stage where the delivered value is less than the payment made, such payment shall be covered by an advance payment guarantee.

17.2 For Support/AMC contracts, KPC PLC shall pay quarterly or annually in arrears unless otherwise specified in the SCC.

17.3 KPC PLC shall effect payment within 30 days of receiving a valid invoice, evidenced by the applicable milestone acceptance certificate.

17.4 KPC PLC shall deduct withholding tax from all payments as required by Kenyan tax law.

18. LIQUIDATED DAMAGES

18.1 If the Vendor fails to achieve any key milestone by the date specified in the Implementation Plan (as extended by agreed Change Requests or Force Majeure), KPC PLC shall be entitled to deduct Liquidated Damages (LD) at the rate stated in the SCC.

18.2 The standard LD rate is 0.5% of the Contract Price per day of delay. The maximum aggregate LD shall not exceed 10% of the Contract Price unless otherwise specified in the SCC.

18.3 Liquidated Damages shall not apply where: delay is caused by KPC PLC's failure to meet its obligations (e.g., delayed access, delayed UAT participation, delayed data provision); or the delay is due to a Force Majeure Event.

19. PERFORMANCE SECURITY

19.1 The Contractor shall provide a Performance Security within ten (10) working days of signing of the award, in the form and amount stated in tender document.

19.2 The Performance Security shall be valid for the entire contract period plus ninety (90) months after issuance of the Final Acceptance Certificate including any and/or all extensions.

19.3 The amount of Performance Security shall be: **10%** of the Contract Sum.

19.4 The Performance Security shall be in the form of the Unconditional Demand Bank Guarantee issued by a reputable tier 1 banks regulated by the Central Bank of Kenya and shall be payable on demand.

19.5 The Performance Security shall not be reduced on the date of the Operational Acceptance.

19.6 The Performance Security proceeds shall be payable to KPC PLC as compensation for any loss resulting from the Contractor's failure to complete its obligations. KPC PLC may call on the Performance Security where the Supplier is in material breach and fails to remedy such breach within fourteen (14) days of written notice.

19.7 KPC PLC shall return the Performance Security to the Contractor within thirty (30) days of completion of the Contract and issuance of the Final Acceptance Certificate.

20. AUDIT RIGHTS

20.1 KPC PLC and its authorised representatives (internal/external auditors, regulators) shall have the right, on 5 working days' notice, to audit the Vendor's records, accounts and processes relating to this Contract, including security controls, licence compliance, SLA performance data and financial records for 7 years from the Contract date.

20.2 Software Licence Audit: KPC PLC reserves the right to audit its own use of licensed software to ensure compliance with licence terms. The Vendor shall provide audit tools or reports to support such audits.

21. CONFIDENTIALITY

21.1 Each Receiving Party shall keep Confidential Information secure, use it only for purposes of the Contract, restrict access to authorised persons with a need to know, and take reasonable steps to prevent unauthorised disclosure, copying, misuse or access.

21.2 Confidential Information may be disclosed only to authorised personnel, advisers, auditors, insurers, financiers, affiliates or approved subcontractors bound by equivalent confidentiality obligations, where required by law or a competent authority, or with the Disclosing Party's prior written consent. The Receiving Party remains responsible for any breach by persons to whom it discloses the information.

21.3 Confidentiality obligations shall not apply to information that is public other than through breach, was lawfully known before disclosure, is lawfully received from a third party without restriction, or is independently developed without reference to the Confidential Information.

21.4 Where Confidential Information includes personal data, each Party shall comply with applicable Kenyan data protection laws and apply appropriate technical and organisational safeguards.

21.5 Confidential Information remains the property of the Disclosing Party and no ownership, licence or intellectual property right is transferred except the limited right to use it for the Contract.

21.6 On expiry, termination or written demand, the Receiving Party shall stop using and return or destroy Confidential Information, except for one archival copy retained where required by law or regulatory compliance.

21.7 A breach may cause irreparable harm, and the Disclosing Party may seek injunctive relief, specific performance or any other remedy available under Kenyan law.

21.8 This Clause survives expiry or termination for five (5) years, while trade secrets and proprietary information remain protected for as long as they retain their confidential nature.

21.9 The Contractor acknowledges that KPC PLC is listed on the Nairobi Securities Exchange and is subject to applicable continuous disclosure obligations under capital markets laws and regulations.

22. FORCE MAJEURE

22.1 A Force Majeure Event means an event beyond the affected Party's reasonable control that was unforeseeable and unavoidable. Force Majeure Events include: acts of God; war; terrorism; earthquake; flood; epidemic or pandemic declared by a competent authority; government-imposed restrictions; or similar events.

22.2 The affected Party shall notify the other within five (5) days of the Force Majeure Event, stating its nature, likely duration, and impact on the Works. Unless otherwise directed by KPC PLC, the Contractor shall continue to perform its obligations as far as reasonably practicable and seek all reasonable alternative means for performance.

22.3 Upon receipt of such notice, the Parties shall determine and agree whether the event qualifies as a Force Majeure event under this Contract.

22.4 If Force Majeure continues for more than ninety (90) days, either Party may terminate the Contract on twenty-one (21) days' written notice. KPC PLC shall pay the Contractor for work properly executed and materials reasonably procured before termination.

22.5 The Contractor shall obtain insurance for all Majeure events where commercially reasonable terms are available in the market.

23. SUSPENSION

23.1 KPC PLC may suspend the Contract by 5 working days' written notice. If the suspension is not due to the Vendor's default and exceeds 30 days, KPC PLC shall compensate the Vendor for proven reasonable standby costs.

24. TERMINATION

24.1 Termination for Vendor Default: KPC PLC may terminate immediately if: (a) the Vendor commits a material breach and fails to remedy within 21 days of notice; (b) the Vendor becomes insolvent; (c) the Vendor engages in corrupt/fraudulent conduct; (d) a critical security breach arises from the Vendor's negligence; (e) aggregate LD reaches 10% of the Contract Price.

24.2 On termination for Vendor default: KPC PLC may call the Performance Security; engage another vendor to complete the project; and recover all additional costs from the defaulting Vendor. The Vendor shall promptly hand over all work-in-progress, source code, data and documentation.

24.3 Termination for Convenience: KPC PLC may terminate the Contract on 30 calendar days' written notice. KPC PLC shall pay for: Deliverables properly received; licences effectively granted; reasonable demobilisation costs. KPC PLC shall not be liable for anticipated profits on uncompleted work.

25. TRANSITION AND EXIT

25.1 At the end of the Contract (whether by expiry, termination for convenience, or non-renewal of support), the Vendor shall provide reasonable transition assistance including: continuing support during the handover period (minimum 90 days); export of all KPC PLC data in agreed formats; knowledge transfer to KPC PLC's team or successor vendor; and release of Escrow Materials if applicable.

25.2 The Vendor shall not hold KPC PLC's data or systems hostage to payment disputes. Even where payment is disputed, the Vendor shall continue essential support for critical systems and provide data export within 30 days of request.

26. LIMITATION OF LIABILITY

26.1 Except in cases of fraud, criminal negligence or wilful misconduct: (a) neither Party shall be liable for indirect or consequential loss (loss of profit, loss of data, loss of business); and (b) the Vendor's aggregate liability under this Contract shall not exceed the total Contract Price. These limitations shall not apply to: IP indemnity obligations; data protection breaches; confidentiality breaches; or cybersecurity incidents caused by the Vendor's negligence.

27. DISPUTE RESOLUTION

27.1 Any dispute shall first be referred to the Engineer for a decision. The Engineer shall issue a written decision within twenty-one (21) days. Either Party may dissatisfy with the Engineer's decision within twenty-one (21) days.

27.2 Disputes not resolved by the Engineer shall be referred to amicable settlement between the KPC PLC General Manager — Supply Chain and the Contractor's designated representative for amicable resolution within twenty-one (21) days of the dispute being referred. KPC PLC and the Contractor shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the contract

27.3 If, after thirty (30) days from the commencement of such informal negotiations both parties have been unable to resolve amicably a contract dispute, either party may refer the matter to a court of competent jurisdiction in Kenya for determination.

27.4 The Contractor shall continue to execute the Works pending resolution of any dispute.

28. NON-SOLICITATION

28.1 During the Contract and for 12 months after its expiry or termination, neither Party shall directly solicit or recruit the other Party's employees who were involved in this Contract, without the prior written consent of the other Party.

29. NON-WAIVER AND SEVERABILITY

29.1 No failure to enforce any provision shall constitute a waiver. Any waiver must be in writing.

29.2 If any provision is invalid or unenforceable, the remainder of the Contract continues in full force.

30. NOTICES

30.1 All notices shall be in writing addressed to the respective Party at the address stated herein below:

For the Procuring Entity:

Attention: Managing Director/CEO

Kenya Pipeline Company PLC

Postal address:73442-00200 Nairobi

Physical Address: Kenpipe Plaza, Sekondi Road

Off Nanyuki Road Industrial Area, Nairobi.

Telephone: (254) 020-2606500-4, 0720207678/9.

Electronic mail address: gmsc@kpc.co.ke and md@kpc.co.ke

Notices shall be deemed received:

a) When delivered personally — on the date of delivery;
b) By recorded/registered courier — upon confirmation of delivery
c) By email — upon receipt of a read receipt or delivery confirmation from the receiving Party's email server, or within two (2) working day of sending if no bounce notification is received.

30.2 Non-Waiver: No relaxation, forbearance, delay or indulgence by either Party in enforcing any provision of this Contract, and no granting of time by either Party to the other, shall prejudice, affect or restrict the rights of that Party under this Contract, nor shall any waiver by either Party of any breach operate as a waiver of any subsequent or continuing breach. Any waiver must be in writing, dated and signed by an authorized representative of the waiving Party.

30.3 Severability: If any provision of this Contract is or becomes illegal, invalid or unenforceable in any jurisdiction, that shall not affect the legality, validity or enforceability of that provision in any other jurisdiction, or the legality, validity or enforceability of any other provision of this Contract.

31. ENTIRE AGREEMENT

31.1 The Contract constitutes the entire agreement and supersedes all prior representations and negotiations. No amendment shall be valid unless in writing and signed by both Parties.

32. ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG) COMPLIANCE

32.1 The Parties shall conduct business sustainably, ethically and responsibly, and shall comply with all applicable environmental, social and governance laws, regulations, standards and policies in Kenya and any other relevant jurisdiction.

32.2 Environmental Obligations

The Supplier shall comply with environmental laws, permits and standards; minimise adverse environmental impacts; use resources efficiently; safely handle, store, transport and dispose of hazardous substances and waste; maintain required licences and permits; and promptly notify KPC PLC of any material environmental incident, regulatory notice or investigation.

32.3 Social Obligations

The Supplier shall comply with labour and employment laws; provide a safe and healthy workplace; prohibit forced labour, child labour, human trafficking, discrimination, sexual harassment, bullying, abuse, and all forms of workplace harassment; promote fair labour practices and equal opportunity; respect human rights; and maintain procedures for workplace grievances and safety complaints.

32.3 Governance and Ethical Conduct

The Supplier shall conduct business with integrity; comply with anti-corruption, anti-bribery, anti-money laundering, fraud prevention, data protection and privacy laws; avoid improper payments or advantages; maintain accurate records and internal controls; safeguard confidential and personal information; and promptly notify KPC PLC of any actual or suspected breach.

32.4 The Supplier shall use reasonable endeavours to ensure that subcontractors, agents and suppliers engaged in the Contract comply with substantially similar ESG standards and shall remain responsible for their acts and omissions.

32.5 KPC PLC may, on reasonable notice, request information or records needed to verify ESG compliance, and the Supplier shall cooperate with such request.

32.6 If the Supplier breaches this Clause, KPC PLC may require a corrective action plan. Failure to remedy the breach within the required period shall constitute a material breach.

32.7 Any serious ESG violation, including corruption, forced or child labour, serious environmental breach or persistent legal non-compliance, shall entitle KPC PLC to suspend performance or terminate the Contract immediately, without prejudice to other remedies.

32.8 This Clause shall survive expiry or termination of the Contract to the extent necessary to address any act, omission, investigation, claim or liability arising during the Contract term.

PART 5 – SPECIAL CONDITIONS OF CONTRACT AND SLA

SECTION VI-A: SPECIAL CONDITIONS OF CONTRACT (SCC) SUMMARY MATRIX AND SLA

These Special Conditions supplement or amend the GCC-IT. The SCC prevails over the GCC-IT in the event of conflict. Complete for each specific IT procurement.

GCC-IT Reference	Special Provision
GCC-IT 2 — Governing Law	Laws of Kenya (as specified in GCC-IT 2.1)
GCC-IT 4 — Scope	Hardware / Software / Licences / Implementation / Support / Managed Services
GCC-IT 4.2 — Approved Subcontractors	No subcontracting without prior written approval
GCC-IT 5.4 — Hardware Replacement Period	Next business day from notification of defect during Warranty Period
GCC-IT 7 — Software Escrow	Not required
GCC-IT 8.2 — Testing Requirements	Unit Testing and System Integration Testing, Disaster Recover Testing
GCC-IT 9 — Acceptance	Performance Acceptance Criteria (PAC): after successful Performance Testing, System Integration Test, User Acceptance Test, and Go-Live. PAC kicks in DLP, Hypercare Period and warranty. Final Acceptance Criteria (FAC): 90 days after PAC, subject to no unresolved P1/P2 bugs Hypercare Period: 90 days from PAC
GCC-IT 12 — Warranty Period	3 Years for Software and 3 Years for Hardware from PAC for hardware and software
GCC-IT 13 — SLA — Refer to SLA Schedule below	To be provided

<table>
<tr><td>GCC-IT 14 — Cybersecurity Standards</td><td>Minimum : ISO/IEC 27001 / SOC 2 Type II
14.2(a) Penetration testing shall be carried out by Quality Assurance Consultant.</td></tr>
<tr><td>GCC-IT 15.3 — Data Residency</td><td>Personally Identifiable Data must reside in Kenya</td></tr>
<tr><td>GCC-IT 16.2 — Custom IP Assignment</td><td>Ownership of Custom Work vests in KPC PLC upon creation and upon full payment</td></tr>
<tr><td>GCC-IT 17 — Payment Schedule</td><td>LOT 1 – Provision of Programme Management Office Services
<table>
<tr><th>No.</th><th>Milestone</th><th>Key Deliverables</th><th>Acceptance Requirement</th><th>Payment (%)</th></tr>
<tr><td>1</td><td>Mobilization and Programme Initiation</td><td>Programme Charter, Programme Governance Framework, Mobilization Plan, Integrated Master Programme Plan and Programme Management Plan</td><td>Stage Gate 1 Approval</td><td>10</td></tr>
<tr><td>2</td><td>Business Requirements and Solution Design</td><td>Design Governance Reports, Architecture Assurance Reports, Design Review Reports and Stage Gate Assessment Report</td><td>Stage Gate 2 Approval</td><td>15</td></tr>
<tr><td>3</td><td>Infrastructure Deployment</td><td>Infrastructure Readiness Reports, Quality Assurance Reports and Contractor Performance Reports</td><td>Stage Gate 3 Approval</td><td>10</td></tr>
<tr><td>4</td><td>Solution Configuration and Development</td><td>Programme Performance Reports, Quality Assurance Reports, Executive Dashboards and Contractor Performance Reports</td><td>Stage Gate 4 Approval</td><td>20</td></tr>
</table></td></tr>
</table>

5	Integration, Testing and Data Migration	Integration Assurance Reports, Migration Assurance Reports, Testing Governance Reports and Readiness Assessment Reports	Stage Gates 5 and 6 Approval	20
6	Go-Live and Hypercare	Go-Live Readiness Assessment, Hypercare Reports, Stabilization Reports and Operational Readiness Report	Stage Gates 7 and 8 Approval	15
7	Programme Closure	Programme Closure Report, Benefits Realization Report, Lessons Learned Report, Knowledge Transfer Completion Report and Final Handover Report	Stage Gate 9 and Final Acceptance	10
Total				**100**

LOT 2- Design, Supply, Implementation, Commissioning, Support and Maintenance of an Enterprise Digital Solution.

#	Payment Milestone	%	Certifiable Milestone Outputs	Acceptance Gate
1	Project Initiation	3%	Project kickoff minutes; Project Charter; Implementation Plan; WBS; detailed schedule; governance framework; project team arrival; risk register; communication/change plan; Data Migration – Strategy, Environment Build & Extraction Readiness Data Object Inventory / migration scope catalogue covering master and transactional data across the legacy TMS, ERP, finance and HR systems. Data quality baseline assessment and cleansing rules agreed	Project Readiness: Project team mobilized; governance approved; project plan baselined; WBS and schedule approved; risks/dependencies registered; project controls operational; formal kickoff completed
2	Infrastructure Delivery to the KPC Site – Inspected and Accepted	12 %	Packing lists; bills of landing or airway bills; certificates of origin; insurance certificates; serial number schedule; goods received note; inspection report confirming no damage and correct configuration against the BOM	Delivery Notes and Acceptance Certificates against the BOM

	3	Infrastructure Installation Integration & Acceptance: completion with site acceptance tests; passed Delivery of Full software licenses entitlements delivered and verified as installed in KPC's development and test environments.	20 %	As-built rack elevations and cabling schedules; power and cooling sign-off; firmware and patch baseline recorded; performance and failover test results against the technical specification; Operational Acceptance Certificate; capacity and performance report at production load. Entitlement certificates issued in the name of Kenya Pipeline Company PLC; licence portal and licence server access transferred to KPC; installation report countersigned by KPC ICT; reconciliation of licence metric and count against the BOQ MOCK 1- Data Migration ETL environment operational with connectivity to all legacy source systems confirmed; data quality baseline complete with cleansing rules	Infrastructure Readiness: All contracted infrastructure installed/configured; connectivity validated; Dev/Test/Training/Pre-Production/ /Production environments operational; backup/restore tested; security hardening completed; performance/capacity tests passed; infrastructure ready to support solution implementation; Infrastructure Acceptance Certificate issued Install Software license: Operational Acceptance Certificate; production instance registered against KPC entitlements Final Acceptance Certificate; licence compliance report demonstrating entitlement equal to or greater than deployment and licence quantities reconciled with the BOQ

	4	Business & Technical Requirements Sign-off Solution Architecture & Detailed Design Approval	5%	Completed As-Is Assessment; To-Be Processes; BRS; FRS; TRS; RTM; Gap Analysis; Data & Integration Requirements Solution Architecture; Application, Data, Integration, Infrastructure & Security Architecture; Disaster Architecture; Detailed Design; Security Design	Requirements Baseline: 100% of agreed business areas/processes assessed; requirements documented and traceable; major gaps resolved/accepted; To-Be processes approved; requirements baseline formally signed off Design Approval: Architecture compliant with approved requirements; security, integration, data and infrastructure designs approved; design review issues resolved; no outstanding critical design issues; Technical Design Authority approval issued
	5	Configuration , Development & Integration Completion	25 %	Configured modules; custom developments; APIs/interfaces; workflows; reports/dashboards; migration scripts; configuration documentation; SIT-ready solution Subscription to Saas deliverable MSOOS/TMS, OT integration and depot systems (five depots)	Build Completion: Agreed functionality configured/developed; interfaces operational; unit testing completed; agreed defects within permitted threshold; RTM demonstrates coverage of requirements; solution technically ready for SIT; Build & Integration Completion Certificate issued

	6	System Integration Testing (SIT) Completion	10 %	SIT plan; test scripts; executed tests; integration results; performance/security testing; defect register; SIT report Mock 2 - Data Migration Testing and Completenes Check ETL/migration environment provisioned, with verified connectivity to all legacy source systems Extraction scripts developed for priority data objects	SIT Acceptance: Agreed SIT test cases executed; critical business/integration scenarios successfully passed; no unresolved Critical defects; High defects resolved or formally accepted with remediation plan; integrations validated; performance/security tests completed; SIT Acceptance Certificate issued Configuration workbooks; unit and integration test results; defect log; development, QA and pre-production environments handed over.

	7	UAT, Training & Operational Readiness	10 %	UAT plan/results; UAT sign-off; training programme; manuals; training records; SOPs; support procedures; operational readiness assessment Reconciliation report for every migrated object, signed by the named data owner; cleansing exception log closed. Mock 3 - Data Migration Testing and Completenes Check ETL/migration environment provisioned, with verified connectivity to all legacy source systems Extraction scripts developed for priority data objects	Business Readiness: UAT successfully completed; business owners sign off; Critical/High defects preventing business operation resolved; agreed users trained; support model operational; SOPs approved; business and operational readiness confirmed; UAT & Operational Readiness Certificate issued SAT passed, including the interface to the ERP; earned individually per depot site. Order-to-cash and terminal operations demonstrated end to end in production for a continuous 30-day period across all five depots.

KPC - Public

8	Production Deployment & Go-Live	5%	Cutover Plan; Data Migration Report; Reconciliation Report; Production Deployment Report; Go-Live Checklist; production validation; support activation	Production Acceptance: Cutover successfully completed; agreed data migrated and reconciled; production environment operational; critical business processes successfully validated; support/helpdesk operational; rollback/contingency arrangements confirmed; authorized Go-Live Certificate issued as agreed end-to-end transaction set processed in production.
9	Hypercare & Stabilization Expiry of Defects Liability Period	5%	Hypercare Report; SLA/KPI Report; Incident & Defect Report; Performance Report; Adoption Report; Stabilization Report; Knowledge Transfer Report	Stabilization: System operating satisfactorily in production for agreed stabilization period; SLA/KPI thresholds achieved; no unresolved Critical defects; High defects within agreed tolerance; incident volumes stabilized; support team demonstrably capable; Stabilization Acceptance Certificate issued Expiry of Defects Liability Period- Certificate of expiry. 12 months from Operational Acceptance elapsed; all warranty defects closed or waived in writing by KPC.

	1 | Final Acceptance, Handover & Knowledge Transfer | 5% | Final Acceptance Report; as-built architecture; technical documentation; configuration records; security/DR documents; O&M manuals; knowledge transfer; asset register; closure report | Final Acceptance: All contractual deliverables accepted; documentation complete; knowledge transfer completed; outstanding defects within agreed warranty/support arrangements; assets and configurations handed over; support/warranty activated; project closure approved; Final Acceptance Certificate issued **All payments shall be made to the Prime Contractor/Lead Firm unless otherwise advised by KPC PLC in writing. Tenderers shall disclose in their tender any OEM licensing compliance requirement (for example, direct licence contracting between the OEM-authorised partner and KPC PLC). The OEM-authorised consortium member shall procure the OEM licences for KPC PLC in compliance with the OEM's licensing regulations.**
GCC-IT 17.2 — Support/AMC Payments	[Quarterly / Annually] in arrears against monthly SLA performance reports
GCC-IT 18 — Liquidated Damages	LD Rate: 0.5% of Contract Price per day of delay Maximum aggregate LD: 10% of Contract Price
GCC-IT 19 — Performance Security	Required: 10% of Contract Price — Bank Guarantee from a tier 1 Bank regulated by the Central Bank of Kenya for the project entire contract period plus 90 days after FAC.
GCC-IT 25 — Transition Assistance	Transition assistance: 90 days from end of contract; KPC PLC retains all data and source code
GCC-IT 26 — Liability Cap	Aggregate liability cap: Total Contract Price
Additional SCC Provisions	[Insert project-specific provisions]

Advance Payment	20% — against advance payment guarantee
OEM Authorisation Required	Yes — for Lot 2
Local Content Preference	Not applicable
Additional Requirements	To be provided

SECTION VI-B: DETAILED SPECIAL CONDITIONS OF CONTRACT -- DESIGN, SUPPLY, IMPLEMENTATION, COMMISSIONING, SUPPORT AND MAINTENANCE OF AN ENTERPRISE DIGITAL SOLUTION (LOT 2)

This Section VI-B forms part of the Special Conditions of Contract (Section VI) and sets out the detailed special conditions specific to Lot 2.

CLAUSE 1: DEFINITIONS AND INTERPRETATION

1.1 In this Contract, unless the context otherwise requires:

Term	Definition
"Programme"	The KPC Enterprise Digital Transformation Programme described in the TENDER and TENDER, comprising the Lot 1 PMO Contract and this Lot 2 Implementation Contract.
"Solution"	The integrated Enterprise Digital Transformation Solution comprising all the solution components in the Scope Schedule, including the ERP/EAM platform, the E-Procurement (Source-to-Pay) platform, the Midstream Oil Operations System and Terminal Management System (MSOOS/TMS), Enterprise Data Platform, Enterprise Integration Platform, cybersecurity integrations, OT integrations, and the Primary Data Centre and DR infrastructure (enterprise-class x86 platforms on enterprise Linux).
"PMO"	The independent Programme Management Office contractor engaged under Lot 1, acting as the KPC PLC's programme governance, planning, monitoring and quality assurance agent, without authority to vary this Contract.
"TOM Approval Gate"	The KPC PLC's written approval of the TOM, before which the Contractor is limited to discovery and planning activities per Clause 4.4.
"Release"	A contractually defined, independently acceptable increment of the Solution (by component, functional scope and/or site) set out in the Release Plan.
"Deployment Wave"	The rollout of an accepted Release to a defined group of sites, depots or user populations.
"OT" / "OT Systems"	Operational technology, including SCADA, terminal automation, DeltaV-based systems, hydrant management, tank gauging, LIMS, PIMS, historians and related pipeline and terminal control and safety systems.
"SaaS Services"	Software provided as a cloud service under this Contract (which may include the Source-to-Pay platform), together with associated hosting, support, and sub-processor services.
"Go-Live Declaration"	The KPC PLC's written confirmation that a Release (or Deployment Wave) is released for productive use.
"Hypercare Period"	Ninety (90) calendar days from each Production Go-Live Declaration (or such longer period stated in the Release Plan for the core ERP Release), with enhanced on-site and remote support at no additional cost.
"Operational Acceptance"	The KPC PLC's written acceptance of the complete Solution after the final Release: all Hypercare Periods closed, all Severity 1 and 2 defects resolved, data migration reconciliations signed off,

	performance benchmarks in Clause 16 achieved, and all documentation delivered.
"Solution Standards"	The minimum solution standards as outlined in the Technical, Functional and Security requirements outlined in this tender, which are incorporated as continuing contractual warranties under Clause 7.
"Critical Infrastructure"	Designated critical information infrastructure within the meaning of the Computer Misuse and Cybercrimes Act, 2018 and regulations thereunder.
"PPADA"	The Public Procurement and Asset Disposal Act, No. 33 of 2015 and the Public Procurement and Asset Disposal Regulations, 2020, each as amended.

CLAUSE 2: SCOPE OF CONTRACT

2.1 The Contractor shall deliver the Solution across all components of the Scope Schedule through the full delivery lifecycle of design, supply, installation, blueprinting (detailed To-Be design), development, testing, data migration, go-live, hypercare and support, for all KPC PLC sites (head office, regional offices, pump stations and depots), including all licences, subscriptions, infrastructure, professional services, training, documentation and knowledge transfer, and multi-year support under Clause 19.

2.1A The delivery lifecycle phases map to the Contract as follows:

Lifecycle Phase	Primary Contractual Provisions
Design	Cl. 4 (TOM gate & governance), Cl. 5 (Requirements Baseline & RTM), Sch. 8 (design acceptance)
Supply	Cl. 8 (licensing), Cl. 9 (SaaS), Cl. 10 (infrastructure), Sch. 3 (licence management), Sch. 6–7 (hardware warranty, rights to use)
Installation	Cl. 10–11 (infrastructure & OT site works), Sch. 8 (M2–M3 certificates)
Blueprinting	Cl. 4.4 (post-TOM detailed To-Be design), Cl. 5.2 (fit-gap discipline), Sch. 8 (M4)
Development	Cl. 5.2 (extensibility standards), Cl. 12 (integrations & ICDs), Sch. 5.3 (custom warranty), Sch. 9 (quality gates)
Testing	Cl. 15–16 (staged acceptance, performance), Sch. 1 (test regime)
Data Migration	Cl. 13 (zero-loss warranty), Sch. 2 (reconciliation standards)
Go-Live	Cl. 14 (cutover & continuity), Sch. 10 (readiness, go/no-go, waves)
Hypercare	Sch. 10.4 (6 months hypercare with exit criteria)
Support	Cl. 19 (SLA), Sch. 4 (roadmap & upgrades), Sch. 11 (defect liability & support term)

2.2 The scope includes translation of the approved requirements into detailed To-Be business processes, workflows, configurations and standard operating procedures; the Contractor shall not modify the approved requirements or governance framework without the KPC PLC's approval through the Programme Steering Committee.

2.3 The Contractor confirms it has examined the KPC PLC's business, sites, legacy landscape and OT environment through the procurement process and **no claim for additional**

payment or time shall be entertained on grounds of insufficient familiarity with the KPC PLC's environment, integration complexity, or the condition of legacy data, save for latent conditions that could not reasonably have been discovered.

CLAUSE 3: SINGLE POINT OF RESPONSIBILITY, CONSORTIUM AND OEM BACK-TO-BACK

3.1 The Contractor assumes **end-to-end, single-point responsibility** for the complete Solution and all components, products, services, interfaces, custom developments, integrations, infrastructure and deliverables, regardless of whether provided directly or through consortium members, subcontractors, OEMs (including the ERP OEM, E-Procurement Provider, MSOOS OEM and Infrastructure OEM), affiliates or other third parties. No failure by any such party shall excuse the Contractor.

3.2 Where the Contractor is a consortium: all members are jointly and severally liable; the Lead Member has authority to bind all members; the composition approved at tender shall not change without the KPC PLC's prior written approval; and each member's scope shall be disclosed in the Consortium Schedule.

3.3 The Contractor shall maintain, and evidence annually, valid OEM authorisations and partnership levels for the ERP OEM, the E-Procurement Provider, the MSOOS OEM, the Infrastructure OEM and the enterprise Unix vendor, at levels entitling it to sell, implement, escalate incidents and obtain roadmap commitments for the KPC PLC. Loss of any such authorisation is a material breach unless a replacement acceptable to the KPC PLC is in place within thirty (30) days.

3.4 The Contractor shall flow down to each OEM and subcontractor obligations no less protective than this Contract in respect of confidentiality, data protection, security, audit, escrow (where applicable), and business continuity, and shall procure for the KPC PLC direct licence confirmations from the ERP OEM and E-Procurement Provider so that the KPC PLC's usage rights survive any failure of the Contractor.

3.5 Where the Contractor is a subsidiary or relies on group covenant strength for the tender, a parent company guarantee in the KPC PLC's form shall be delivered within fourteen (14) days of award as a condition precedent.

CLAUSE 4: PROGRAMME GOVERNANCE AND INTERFACE WITH THE LOT 1 PMO

4.1 The Programme is governed by the KPC PLC through the Programme Steering Committee, supported by the PMO. The Contractor shall comply with the programme governance framework, reporting cadence, stage-gate criteria, RAID management, dependency management, and document standards established under Lot 1 and approved by the KPC PLC.

4.2 The PMO acts as the KPC PLC's agent for coordination, monitoring and quality assurance only. The PMO has no authority to instruct variations, accept deliverables, waive requirements, or relieve the Contractor of any obligation; only the KPC PLC's authorised officer may do so in writing. The Contractor shall not rely on any PMO communication as

a variation, and shall promptly notify the KPC PLC where it considers any PMO direction to have cost, time or scope impact.

4.3 The Contractor shall cooperate fully and in good faith with the PMO, including timely provision of plans, schedules in the agreed toolset, progress data, risk registers, quality records and access to personnel; shall participate in a tripartite interface protocol (KPC PLC–PMO–Contractor) to be executed at mobilisation; and shall not be entitled to claim delay or cost arising from reasonable PMO assurance activities conducted in accordance with that protocol.

4.4 Until the requirements Approval Gate, the Contractor shall confine its activities to mobilisation, discovery, current-state analysis, solution planning, environment establishment and infrastructure works. **Detailed To-Be process design and system configuration shall commence only after the KPC PLC approves the requirements.** The Implementation Schedule shall reflect this sequencing; requirements approval delay beyond the scheduled date is an KPC PLC-risk event entitling the Contractor to extension of time (but not additional cost for the first [30] days of delay).

4.5 Any material deviation from the approved requirements identified during design or configuration shall be routed through the PMO for review and approved by the KPC PLC through the Steering Committee before implementation.

4.6 Disputes between the Contractor and the PMO regarding programme-level direction shall be escalated to the Steering Committee within seven (7) days and shall not suspend performance.

CLAUSE 5: REQUIREMENTS BASELINE AND TRACEABILITY

5.1 The TENDER requirements, the Solution Standards, the approved TOM, and the Contractor's accepted Tender together form the Requirements Baseline. The Contractor shall maintain a Requirements Traceability Matrix (RTM) mapping every requirement to design, build, test case and acceptance evidence, kept current in the programme toolset and auditable by the PMO.

5.2 Fit-gap outcomes shall favour standard product capability: configuration over customisation, and customisation only with the KPC PLC's approval supported by a lifecycle cost and upgrade-impact assessment. All customisations, extensions and integrations shall be built using the OEMs' supported extensibility frameworks so as not to impair upgradeability or OEM support.

5.3 Functionality demonstrated in the Tender or in solution demonstrations, and functionality described in OEM documentation for licensed modules, is deemed in scope at no additional cost, whether or not itemised in the BoM.

CLAUSE 6: CONTRACTOR PERSONNEL

6.1 The Contractor shall deploy the Key Personnel evaluated at tender (Programme Director; Solution Architect; ERP Functional Leads; Technical Lead; Data Migration Lead; Change Management Lead; Cybersecurity Lead; and OT Delivery Lead), each meeting the qualification minima of the TENDER. Key Personnel shall not be replaced without the KPC

PLC's prior written consent; replacements shall have equal or superior qualifications and shall complete a paid handover of not less than ten (10) working days. Unauthorised replacement attracts liquidated damages of [KES 500,000] per occurrence.

6.2 Personnel deployed on OT Systems shall hold current MSOOS OEM certifications and shall comply with the KPC PLC's HSE inductions, permit-to-work system, and site rules at all pump stations and depots. The KPC PLC may require removal of any person for misconduct, security or safety grounds without liability.

6.3 The Contractor shall maintain the local delivery capability represented at tender, including a registered Kenyan presence and qualified local technical resources, for the duration of the Contract, and shall implement the skills and knowledge transfer plan in Clause 18.

CLAUSE 7: SOLUTION STANDARDS AS CONTINUING WARRANTIES

7.1 The Contractor warrants, at Go-Live of each Release and continuously during the support term, that the Solution conforms to the Solution Standards, including that:

(a) The ERP platform is a current OEM-supported release, deployable on-premise or in-country cloud, with segregated DEV, TST, UAT and PRD environments and an OEM-supported roadmap of not less than ten (10) years;

(b) The Midstream Oil Operations System and Terminal Management System contain no End-of-Life or End-of-Support components and carry an OEM roadmap of at least ten (10) years;

(c) All infrastructure components are from the Infrastructure OEM's current Generally Available portfolio, are not EOL/EOS, carry at least three (3) years OEM-backed Next Business Day on-site support in Kenya, and have an active OEM support lifecycle of at least five (5) years from commissioning;

(d) Critical workloads achieve RPO $\leq$ 30 minutes and RTO $\leq$ 2 hours, demonstrated by DR tests before Go-Live and quarterly after Hypercare;

(e) Security controls align to ISO/IEC 27001:2022 and, for OT-connected elements, IEC 62443; comprehensive audit trails, Segregation of Duties and SIEM integration are provided;

(f) The HCM/payroll capability supports Kenyan statutory payroll and future legislative updates within maintenance;

(g) Interoperability is provided through standards-based APIs (REST, SOAP, OData or equivalent); identity integration supports SSO, MFA, SAML 2.0, OAuth 2.0, OpenID Connect, SCIM and LDAP with the KPC PLC's IAM platform; and data is protected with TLS 1.2+ in transit and AES-256 at rest;

(h) Any AI/ML capability is commercially supported, explainable, auditable and securely governed, and no KPC PLC data shall be used to train public or cross-customer AI models without the KPC PLC's written approval; and

(i) A Secure Software Development Lifecycle is applied across the solution lifecycle, with vulnerability management, patching and penetration testing support.

7.2 Breach of a Solution Standard discovered at any time shall be remediated at the Contractor's cost, including replacement of non-conforming components, without prejudice to the KPC PLC's other remedies.

CLAUSE 8: SOFTWARE LICENSING, METRICS AND PRICE PROTECTION

8.1 All licences and subscriptions (ERP, EAM, MSOOS/TMS, data and integration platforms, databases, operating systems, middleware and tools) shall be registered in the KPC PLC's name, sized for the user counts and volumes in the BOM, and shall include all non-production environments (DEV, TST, UAT, training, DR) without additional charge.

8.2 For each product, the licence metric (named user, concurrent user, enterprise, consumption or module basis), included modules, and any usage caps shall be exhaustively stated in the Licence Schedule. Functionality reasonably necessary to operate the contracted business processes shall be deemed included; metric ambiguities shall be construed in the KPC PLC's favour.

8.3 Subscription and support pricing shall be fixed for the initial term of six (6) years from first Production Go-Live, with renewal escalation thereafter capped at the lower of 5% per annum or published OEM list uplift.

8.4 Licence audits: no OEM or Contractor audit shall be conducted more than once in any twelve (12) months, on not less than thirty (30) days' notice, during business hours, using tools approved by the KPC PLC, subject to confidentiality, and never in a manner accessing production data. Any true-up shall be at contracted unit rates without retroactive penalties where the KPC PLC's use was in good faith.

8.5 Enterprise Unix subscriptions with 24x7 production support shall be provided for all instances (including DR and non-production) for the full support term. For all open-source components embedded in the Solution, the Contractor warrants licence compliance and shall provide, on request, a software bill of materials (BoM).

CLAUSE 9: SAAS SERVICES: SOVEREIGNTY, CONTINUITY AND EXIT

9.1 For any SaaS element, the Contractor shall disclose and keep current: hosting locations (primary and DR), cloud providers, sub-processor list, data residency arrangements, and certifications (ISO/IEC 27001 and SOC 2 Type II or equivalent). Changes to hosting regions or material sub-processors require sixty (60) days' prior notice and, where personal data transfer conditions under the Data Protection Act, 2019 are affected, the KPC PLC's approval.

9.2 SaaS availability shall not be less than 99.5% per month with the OEM's standard credits passed through to the KPC PLC in addition to (not in substitution for) the Contractor's SLA obligations in Clause 19. Planned maintenance shall be scheduled outside East Africa business hours where the platform permits.

9.3 Integration between SaaS and on-premise components (ERP, EDRMS, data platform) is the Contractor's end-to-end responsibility, including middleware, API versions, and impact management of SaaS release cycles; SaaS quarterly releases shall be regression-tested against KPC PLC-critical integrations under the support services.

9.4 On expiry or termination of any SaaS element, the Contractor shall procure: (a) continued read access for at least ninety (90) days; (b) **a complete export of the KPC PLC's data, attachments, master data and transaction history in documented, machine-readable formats at no charge beyond media costs**; and (c) certified deletion thereafter. Fees shall never be leveraged to withhold the KPC PLC's data.

CLAUSE 10: INFRASTRUCTURE SUPPLY AND VENDOR-OWNED SIZING

10.1 The Contractor shall supply, install and commission the Primary Data Centre and DR infrastructure (compute, storage, virtualization/containers, databases, load balancing, observability) on enterprise-class x86 platforms running enterprise Unix, delivered DDP (Incoterms 2020), brand new, genuine, from the OEM's authorised Kenya channel, with serial numbers registered to the KPC PLC. DOA units shall be replaced new within fourteen (14) days.

10.2 Sizing risk rests with the Contractor: the infrastructure shall support the full Solution at the contracted user counts and data volumes, plus [30] % growth headroom over Six (6) years, while meeting the performance benchmarks in Clause 16. **If capacity proves insufficient to meet those benchmarks at contracted volumes at any time before the end of the warranty period, the Contractor shall supply and commission additional capacity at no cost to the KPC PLC**.

10.3 Title passes on delivery and payment. Hardware warranty: OEM-backed, minimum three (3) years 24x7 with Next Business Day on-site response in Kenya, running from commissioning, extendable at pre-agreed rates for years four and five.

CLAUSE 11: OT SYSTEMS, SITE WORKS AND OPERATIONAL SAFETY

11.1 Works on or connected to OT Systems (MSOOS, TMS, SCADA interfaces, terminal automation, tank gauging, hydrant systems, historians) shall be performed under the MSOOS OEM's certified methods and the KPC PLC's Management of Change (MOC), permit-to-work and HSE procedures. No connection to, or modification of, any live operational system shall occur without an approved MOC and a rollback plan.

11.2 The KPC PLC's pipeline and terminal operations take absolute precedence. Commissioning on live sites shall occur only within KPC PLC-approved outage or low-activity windows; **the Contractor shall have no claim for standing time or delay arising from operational, safety or security suspensions of site access**, provided the KPC PLC uses reasonable endeavours to provide alternative windows.

11.3 IT/OT integration shall comply with IEC 62443 zones and conduits, the KPC PLC's OT firewall and data-diode architecture, and unidirectional data flows where designated; no direct internet exposure of OT assets shall be introduced. All OT interface designs require the KPC PLC's OT security approval before build.

11.4 **Any incident caused by the Contractor affecting pipeline or terminal operations shall be reported immediately, investigated jointly, and remediated at the Contractor's cost; the Contractor's liability for physical damage and third-party claims arising from such incidents is addressed in Clause 24.**

CLAUSE 12: INTEGRATION RESPONSIBILITIES AND THIRD-PARTY DEPENDENCIES

12.1 The Contractor shall deliver all integrations in the Integration Register (enterprise applications, OT, banking and payment gateways, KRA and other revenue authorities, government and regulatory agencies, identity providers, customer and supplier platforms), each governed by an Interface Control Document (ICD) approved by the KPC PLC, using the Enterprise Integration Platform and documented, supported APIs.

12.2 Where an integration depends on a third party outside either party's control (e.g., a regulator or bank), the Contractor shall complete its side to the published specification and support joint testing; delay solely attributable to the third party is a shared-risk event managed through the change control process with extension of time but no additional Contractor profit.

12.3 **All integrations, custom objects and reports shall be delivered with source artefacts, deployment scripts and documentation sufficient for the KPC PLC or a successor to maintain them and shall vest per Clause 23.**

CLAUSE 13: DATA MIGRATION AND QUALITY

13.1 The Contractor warrants **zero loss and zero corruption of in-scope data and metadata** migrated from the KPC PLC's legacy systems and repositories. Migration shall follow an approved Data Migration Plan with profiling, cleansing rules approved by data owners, mapping specifications, mock migrations (minimum two (2) full mocks for the core ERP Release), and cutover reconciliation.

13.2 Reconciliation evidence per object and source shall include record counts, control totals (including financial balances signed off by Finance), checksum or hash verification for document content, and sampled field-level accuracy of not less than 99.5%, jointly signed off before Go-Live of the relevant Release.

CLAUSE 14: CUTOVER AND BUSINESS CONTINUITY

14.1 Each Production cutover shall be executed under an KPC PLC-approved runbook with rehearsed timings, go/no-go checkpoints held by the KPC PLC, a tested rollback plan, and business continuity arrangements ensuring that pipeline scheduling, terminal loading, billing and payroll are not interrupted beyond the approved cutover window.

14.2 Overrun of an approved cutover window attracts liquidated damages. Invocation of rollback does not relieve the Contractor of the obligation to complete cutover at a rescheduled window at no additional cost.

CLAUSE 15: TESTING AND STAGED ACCEPTANCE

15.1 Acceptance is staged per Release: (a) environment readiness; (b) System Integration Testing exit; (c) User Acceptance Testing exit (test cases traced to the RTM, executed with KPC PLC users); (d) performance, security (including independent penetration test), DR and accessibility test exits; (e) data migration reconciliation sign-off; (f) Go-Live Declaration; and (g) Release acceptance at Hypercare exit. Operational Acceptance follows the final Release per Clause 1.1.

15.2 For OT-related components, factory acceptance testing (FAT) may be conducted at the MSOOS OEM's or Contractor's facility and site acceptance testing (SAT) at each depot shall precede connection to live systems.

15.3 Defects are classified by severity per Clause 19; no stage shall be certified with open Severity 1 or 2 defects in that stage. Productive use, partial use, or lapse of time shall not constitute deemed acceptance; only the KPC PLC's written certificates effect acceptance. The PMO may witness all test stages and audit test evidence.

CLAUSE 16: PERFORMANCE GUARANTEES

16.1 At contracted user counts and data volumes, measured over a representative twenty (20) business-day window:

Benchmark	Guaranteed Target
Interactive ERP transaction response	≤ 2 seconds at the 95th percentile (excluding WAN latency)
Terminal/TMS gate and loading transactions	≤ 2 seconds at the 95th percentile; ANPR read-to-decision ≤ 3 seconds
Critical batch and interfaces	Within agreed batch windows; no critical interface backlog > 15 minutes
Month-end financial close critical path	≤ agreed baseline duration in the Release acceptance criteria
Analytics/dashboard refresh	Executive dashboards ≤ 10 seconds; standard reports ≤ 30 seconds at P95
Availability architecture	No single point of failure; component failover ≤ 15 minutes
DR (critical workloads)	RPO ≤ 30 minutes; RTO ≤ 2 hours, demonstrated by test

16.2 Benchmark failure obliges remediation at the Contractor's cost (tuning and, where necessary, additional software or infrastructure capacity per Clause 10.2) until achieved; the relevant acceptance shall be withheld meanwhile.

CLAUSE 17: CYBERSECURITY AND CRITICAL INFRASTRUCTURE OBLIGATIONS

17.1 The Contractor acknowledges the KPC PLC operates Critical Infrastructure and shall comply with the Computer Misuse and Cybercrimes Act, 2018 (including critical information infrastructure directives), the KPC PLC's ICT and OT security policies, and ISO/IEC 27001:2022-aligned controls throughout delivery and support.

17.2 Contractor access shall be via named accounts through the KPC PLC's IAM/PAM platforms with MFA, least privilege, session recording for privileged access, and immediate revocation on role change; remote access only via KPC PLC-approved channels; no shared accounts, personal devices on production networks, or unsanctioned data extraction.

17.3 The Contractor shall: maintain an SSDLC with code scanning for custom developments; remediate critical vulnerabilities within seven (7) days and high within thirty (30) days of patch availability or disclosure; support quarterly patching cycles across the stack; and cooperate with independent penetration tests before each Go-Live and annually, remediating high/critical findings before Go-Live or within thirty (30) days respectively.

17.4 Security incidents affecting the Solution or KPC PLC data shall be notified to the KPC PLC within twenty-four (24) hours of awareness (and immediately for incidents affecting OT), with full cooperation in investigation, regulatory reporting (including to the Office of the Data Protection Commissioner and sector regulators), forensics and remediation at the Contractor's cost where attributable to it.

CLAUSE 18: TRAINING, CHANGE MANAGEMENT AND KNOWLEDGE TRANSFER

18.1 The Contractor shall deliver the training plan approved at design stage: administrator and technical training (including OEM certification-track seats per the BOM), functional super-user training, end-user training via train-the-trainer with role-based materials, and OT operator/maintainer training at site, coordinated with the Lot 1 change management workstream.

18.2 A structured knowledge transfer programme (shadowing, joint operations during Hypercare, documented runbooks) shall enable the KPC PLC's teams to operate first-line support by Operational Acceptance. Complete as-built documentation, configuration workbooks, ICDs, operations manuals and DR runbooks are preconditions to Operational Acceptance and vest in the KPC PLC.

CLAUSE 19: SUPPORT SERVICES AND SERVICE LEVELS

19.1 The Contractor shall provide support and maintenance for [36] months from Operational Acceptance (with per-Release interim support from each Go-Live), covering all Solution components, integrations and infrastructure, on 24x7 for Severity 1 and 2, with a single service desk, named Service Delivery Manager, ITIL-aligned processes, and quarterly service and capacity reviews attended by the PMO during the programme period.

19.2 Severity, response and resolution targets:

Severity	Definition	Response	Resolution / Workaround
Severity 1	Solution or critical component down (ERP, MSOOS/TMS, integration platform); terminal loading or billing stopped; data corruption; security breach	15 minutes, 24x7	4 hours
Severity 2	Major function severely degraded; DR protection lost; critical interface down (bank, KRA, OT)	30 minutes, 24x7	8 hours
Severity 3	Non-critical function impaired; workaround available	4 business hours	5 business days
Severity 4	Service request, query, cosmetic issue	8 business hours	10 business days

19.3 Availability: Production ERP, MSOOS/TMS and integration platform each **99.9% measured monthly** (SaaS per Clause 9.2), excluding approved maintenance. Service credits: 10% of the monthly support charge for availability 99.5–99.9%; 20% for 99.0–99.5%; 30% below 99.0%; 5% per Severity 1 and 2.5% per Severity 2 resolution breach;

capped at 50% of the monthly charge. Three (3) consecutive months (or four (4) in any rolling twelve (12)) below 99.0% on any critical component is material breach.

19.4 Support includes all updates, upgrades, security patches, statutory payroll and tax updates (MS8), SaaS release regression testing (Clause 9.3), one coordinated full-stack patching cycle per quarter, and maintenance of the RTM, ICDs and as-built documentation as the Solution evolves.

CLAUSE 20: LIQUIDATED DAMAGES FOR DELAY

Refer to Clause 18 of GCC

CLAUSE 21: PAYMENT, CURRENCY AND PRICE BASIS

21.1 Payment is strictly against KPC PLC-certified milestones and acceptances. Indicative structure: As per special condition of contact GCC-IT 17 payment schedule. Licences/subscriptions and support are paid per the Licence and SLA Schedules, support quarterly in arrears net of service credits. No advance payment except against an unconditional advance payment guarantee.

21.2 Prices are firm and fixed for the implementation scope; no cost-of-living, exchange-rate or input-cost adjustment applies. Foreign-currency components, if any, are payable at the exchange rate mechanism stated in the SCC; the Contractor bears FX risk on its supply chain. Taxes and duties are per the Incoterm and Kenyan law; the Contract Price is inclusive of all applicable taxes.

21.3 Invoices are payable within thirty (30) days of a correct invoice supported by the relevant certificate. The KPC PLC may set off liquidated damages, service credits and amounts owed by the Contractor.

CLAUSE 22: CHANGE CONTROL AND VARIATIONS

22.1 Changes to scope, TOM, Release Plan, or contract terms are valid only through the Programme change control process, recommended by the PMO where programme-impacting, approved in writing by the KPC PLC's authorised officer, and compliant with PPADA statutory limits on contract variation. Rate cards for changes are fixed in the Rate Card Schedule for the full term.

CLAUSE 23: INTELLECTUAL PROPERTY

23.1 Configurations, customisations, integrations, reports, data models, ICDs, documentation and all deliverables produced for the KPC PLC vest in the KPC PLC on payment; OEM products remain the OEMs', licensed per Clause 8; Contractor background IP is licensed to the KPC PLC perpetually and royalty-free for use with the Solution. The Contractor indemnifies the KPC PLC against third-party IP claims arising from supplied items.

CLAUSE 24: INDEMNITIES AND LIMITATION OF LIABILITY

24.1 Subject to Clause 23.1, The Contractor indemnifies the KPC PLC against claims, losses and costs arising from: IP infringement; breach of data protection, confidentiality or security obligations; death, personal injury, or physical damage to property (including

pipeline and terminal assets) caused by the Contractor; environmental damage caused by the Contractor's site activities; and fraud or wilful misconduct.

24.2 Subject to Clause 24.3, aggregate liability is capped at 100% of the Contract Price; neither party is liable for loss of profit or purely consequential loss, save that the KPC PLC's demonstrable revenue losses from terminal loading or pipeline billing stoppage caused by Contractor default are direct losses recoverable up to 100% of the contact value.

24.3 No cap or exclusion applies to: the indemnities in Clause 24.1; breach of the zero-data-loss warranty; Environmental damage; Public liability; abandonment; fraud; or wilful default. LDs and service credits count toward but do not exhaust the cap.

24.4 The contractor shall put in place WIBA and all risk insurance cover for Environmental liability and Public liability

CLAUSE 25: DATA PROTECTION, ETHICS AND LOCAL CONTENT

25.1 The Contractor shall comply with the Data Protection Act, 2019 (executing the KPC PLC's Data Processing Agreement as a condition precedent), the Access to Information Act, 2016 as applicable, the Bribery Act, 2016, the Anti-Corruption and Economic Crimes Act, 2003, PPADA integrity provisions, and the KPC PLC's Code of Ethics. KPC PLC data shall be hosted and processed in Kenya except if expressly disclosed and approved under Clause 9.1.

25.2 The Contractor shall implement the local content commitments made at tender, including Kenyan professional participation and skills transfer, reported semi-annually, without derogating from certification requirements.

CLAUSE 26: TERMINATION, STEP-IN AND EXIT

26.1 The KPC PLC may terminate for default on: material breach unremedied within fourteen (14) days of notice; exhaustion of maximum LDs; contractors negligence; A critical security/cybersecurity breach caused by Contractor negligence persistent; SLA failure (Clause 19.3); insolvency of the Contractor or a consortium Lead Member; debarment by any organization; loss of a critical OEM authorisation unremedied under Clause 3.3; or prohibited practices under any laws. Termination may be of the whole Contract or, at the KPC PLC's election, of affected components or Releases only, with an equitable price adjustment.

26.2 Step-in: on a Severity 1 situation persisting beyond resolution targets, or Contractor suspension of work without entitlement, the KPC PLC may after 30 days' notice (itself or through third parties, including the OEMs directly) take reasonable steps to restore service at the Contractor's cost which will be recovered from the contractor's dues , without terminating and without relieving the Contractor of its obligations or voiding OEM warranties.

26.3 Termination for convenience: thirty (30) days' notice; payment for work performed and accepted plus reasonable, evidenced, unavoidable committed costs; no loss of profit on unperformed work.

26.4 Exit: on expiry or any termination the Contractor shall provide up to ninety (90) days' exit assistance at contracted rates, deliver all work-in-progress, credentials, documentation, BoMs, procure SaaS data export per Clause 9.4, support licence novation or direct OEM relationships, and certify sanitisation (NIST SP 800-88) of KPC PLC data on Contractor media. No lien, licence suspension or technical lock shall ever be applied against the KPC PLC's data or operations.

SCHEDULE 1: TESTING (TENDERER TO PROVIDE ALTERNATIVE)

1.1 Test Strategy and Governance

1.1.1 The Contractor shall deliver, within ninety (90) days of the requirements Approval Gate, a Master Test Strategy for KPC PLC approval covering all test stages, environments, tools, data, entry/exit criteria, defect management, regression approach (automated where feasible), OT test safety, and roles. The PMO shall provide independent test assurance and may witness any test and audit any evidence.

1.1.2 All test cases shall trace to the Requirements Traceability Matrix (RTM). Test coverage shall include 100% of contracted requirements, all interfaces in the Integration Register, all migrated data objects, all custom developments, and negative/exception paths for financially significant and safety-related transactions.

1.1.3 Test data: production data used in non-production environments shall be minimised and pseudonymised/anonymised per the Data Protection Act, 2019, except where UAT and migration testing reasonably require production-representative data under KPC PLC-approved controls.

1.2 Test Stages, Entry/Exit Criteria and Indicative Durations

Stage	Purpose / Scope	Entry Criteria (key)	Exit Criteria (key)
Unit / Configuration Test	Contractor verification of each configuration unit, custom object (RICEFW) and report	Approved functional/technical design; build complete	100% units passed; peer review records; code scan clean for customs
System Test	End-to-end within each component (ERP, E-Procurement, MSOOS/TMS, data platform)	Unit test exit; environment & test data ready	All planned cases run; zero Sev1/Sev2 open; Sev3 with agreed plan
System Integration Test (SIT)	Cross-component and external interfaces (banks, KRA, OT, IAM) per ICDs	System test exit; stubs/partners ready; ICDs approved	100% interfaces proven incl. failure/replay paths; zero Sev1/Sev2
Data Migration Mock Tests	Full-volume mock loads with reconciliation (see Schedule 2)	Cleansed extracts; mapping specs approved	Reconciliation within tolerance; timing fits cutover window
Performance & Volume Test	Clause 16 benchmarks at contracted volumes +30% headroom	SIT exit; production-scale environment	All benchmarks met at P95; capacity report accepted

Security Testing	Vulnerability assessment + independent penetration test; SoD ruleset validation	SIT exit; hardening applied	No open critical/high findings; SoD conflicts resolved or risk-accepted by KPC PLC
DR / Resilience Test	Failover, failback, backup-restore, RPO≤30min / RTO≤2h proof	Performance exit; DR replication live	DR criteria demonstrated and witnessed; runbooks accepted
OT FAT	Factory acceptance of MSOOS/TMS and OT interfaces at OEM/staging facility	Approved FAT protocol; simulation harness	FAT protocol passed and signed; punch list ≤ agreed threshold
OT SAT	Site acceptance per depot before live connection, under MOC/permit-to-work	FAT exit; MOC approved; rollback plan	SAT protocol passed per site; no impact on live operations
User Acceptance Test (UAT)	KPC PLC business users execute business scenarios end-to-end	SIT exit; training of testers; UAT scripts approved	100% scripts executed; zero Sev1/Sev2; KPC PLC UAT certificate
Regression (per change/patch)	Protect accepted functionality incl. quarterly SaaS releases	Baselined automated pack	Pack passed; failures resolved before deployment

1.2.1 Indicative durations per Release: System Test [4] weeks; SIT [6] weeks; Performance/Security/DR [4] weeks in parallel where safe; UAT [6] weeks including one (1) re-test cycle. UAT for R1 shall include a full month-end and payroll simulation; UAT for R3 shall include a full terminal loading day simulation per pilot depot.

1.3 Defect Management in Testing

1.3.1 Defects are classified per the SLA severity definitions applied to test context. The Contractor shall triage within one (1) business day and fix within: Sev1 – three (3) days; Sev2 – five (5) days; Sev3 – ten (10) days during test phases. A defect re-opened more than twice escalates to the Steering Committee with root-cause analysis.

1.3.2 Test stage exit requires: zero open Severity 1 and 2 defects in that stage's scope; Severity 3 defects not exceeding [15] with an KPC PLC-approved remediation plan; and all evidence (logs, results, RTM coverage report) filed in the programme repository. Exit is effected only by the KPC PLC's written stage certificate (Schedule 12).

SCHEDULE 2: DATA MIGRATION (TENDERER TO PROVIDE ALTERNATIVE)

2.1 Approach and Phases

2.1.1 Migration proceeds per source and per Release through: (a) discovery and profiling; (b) data quality assessment and cleansing (cleansing rules approved by KPC PLC data owners; cleansing executed in source or staging, never silently in flight); (c) mapping specifications to the target model and enterprise Master Data standards; (d) build of repeatable, logged

migration routines; (e) mock migrations; (f) dress rehearsal integrated with the cutover runbook; (g) production cutover; (h) post-load validation and reconciliation sign-off.

2.1.2 Minimum mock cycles: **two (2) full-volume mocks per Release plus one (1) dress rehearsal** (R1 financial objects: three (3) mocks including a trial balance tie-out). Each mock produces a timed log usable for cutover planning and a reconciliation report against Schedule 2.3 tolerances.

2.2 Scope of Objects (indicative)

2.2.1 Master data (chart of accounts, vendors incl. E-Procurement supplier records, customers, employees, assets/functional locations, materials, tariffs); open transactional data (open POs and contracts, open AR/AP, open work orders, in-transit stock, unbilled shipments); balances (GL balances, fixed asset registers with depreciation history, inventory balances, payroll YTD); historical data per the agreed retention strategy (loaded, archived to the data platform, or retained read-only in legacy); and documents/records into EDRMS with metadata and fixity per the EDRMS clauses.

2.3 Reconciliation Standards and Tolerances

Object Class	Reconciliation Method	Tolerance / Standard
Financial balances (GL, AR, AP, FA)	Trial balance and sub-ledger tie-out source vs target, per company/period	Zero variance; Finance sign-off mandatory
Open transactions	Count + value control totals per object per company	Zero unexplained variance; exceptions register for KPC PLC decision
Master data	Counts + field-level sample audit per object	≥ 99.5% field accuracy; 100% of critical fields
Inventory & hydrocarbon stock	Quantity and valuation tie-out per depot/tank at freeze point	Zero variance vs physical/legacy records at cutover
Payroll	Parallel run of [2] payroll cycles vs legacy	Net pay & statutory deductions variance = zero (rounding only)
Documents / records (EDRMS)	Object counts, byte counts, SHA-256 fixity, metadata completeness	100% fixity match; ≥ 99.5% metadata completeness

2.3.1 Reconciliation sign-off per Release is a joint certificate signed by the Contractor Data Migration Lead, the KPC PLC data owner(s), KPC PLC Finance (for financial objects), and witnessed by the PMO; it is a precondition to the Go-Live Declaration of that Release (Schedule 10).

2.3.2 The zero-data-loss warranty in the SCC applies: legacy sources preserved read-only for ninety (90) days after Operational Acceptance; migration-attributable defects discovered within twelve (12) months of the relevant Go-Live remediated (including data reconstruction) at the Contractor's cost.

SCHEDULE 3: LICENCE MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE)

3.1 Licence Register: the Contractor shall establish at mobilisation, and maintain until the end of the support term, a consolidated Licence Register recording, for every software item (ERP modules, E-Procurement subscriptions, MSOOS applications, databases, Linux subscriptions, middleware, tools): product and version, licence metric and quantity, entitlement document reference, environments covered, support/subscription expiry, and assigned owner. The Register is reviewed at each quarterly service review and is auditable by the KPC PLC and PMO.

3.2 Deployment against entitlement: the Contractor shall measure actual consumption against entitlement quarterly using OEM-approved tooling, report variances, and rebalance allocations (e.g., named-user reassignments, module re-allocations) at no cost. If a shortfall arises from Contractor sizing or scoping error, the Contractor procures the shortfall at its cost; if from KPC PLC growth beyond BOM quantities, at the contracted unit rates.

3.3 True-up and audit protocol (per SCC Clause 8.4): maximum one audit per twelve (12) months, thirty (30) days' notice, approved tools, no production data access, true-up at contracted rates, no retroactive penalties for good-faith use. The Contractor shall manage and front all OEM audit interactions.

3.4 Renewals: the Contractor shall give one hundred and twenty (120) days' notice before any subscription/support expiry with renewal quotations at protected pricing (fixed for six (6) years, being two three-year terms, from first Production Go-Live; thereafter capped per the SCC). Lapse of any entitlement due to Contractor omission, and any resulting reinstatement fees, are at the Contractor's cost.

3.5 Non-production and DR use, evaluation sandboxes, and disaster invocation use are included entitlements and shall never trigger additional fees. The Contractor shall deliver an SBOM per Release and warrant open-source licence compliance.

SCHEDULE 4: PRODUCT ROADMAP AND UPGRADE POLICY (TENDERER TO PROVIDE ALTERNATIVE)

4.1 Roadmap warranties (per Solution Standards MS1/MS2/MS4): ERP and MSOOS/TMS platforms carry OEM-supported roadmaps of not less than ten (10) years from Contract signature; no component delivered is End-of-Life or End-of-Support; infrastructure is current-GA with ≥ five (5) years OEM support lifecycle from commissioning.

4.2 Annual roadmap briefing: the Contractor shall convene, each contract year, OEM roadmap briefings (ERP, E-Procurement, MSOOS, infrastructure and operating-system OEMs) for the KPC PLC covering release cadence, deprecations, security direction and upgrade windows, with a written Solution Roadmap Report recommending the KPC PLC's upgrade path for the following twenty-four (24) months.

4.3 Version currency: throughout the support term the Solution shall be maintained within OEM mainstream (not extended) support. Minor releases/patches are applied in the quarterly cycles; one (1) major version upgrade per platform within the support term, where released by the OEM, is included in the Contract Price up to [x] person-days per platform, executed with full regression per Schedule 1.

4.4 EOL protection: if an OEM announces EOL/EOS affecting any component such that the roadmap warranty in 4.1 would be breached, the Contractor shall, at its cost, propose and (with KPC PLC approval) implement a like-for-like supported replacement, including migration and retesting, with no degradation of function or performance.

4.5 Custom developments shall be built only on OEM-supported extensibility frameworks so that they survive upgrades; any custom object broken by an OEM release within the support term is repaired by the Contractor at no cost.

SCHEDULE 5: SOFTWARE WARRANTIES (TENDERER TO PROVIDE ALTERNATIVE)

5.1 The Contractor warrants that all software (OEM and custom): (a) conforms to the Requirements Baseline, its documentation and the Solution Standards; (b) is the current, genuine, properly licensed version; (c) contains no undisclosed open-source obligations that would compel disclosure of KPC PLC configurations; (d) contains no viruses, malware, time-bombs, licence-disabling devices or undisclosed remote-access mechanisms — and no lock, disablement or degradation shall ever be applied against the KPC PLC, including in a fee dispute; (e) does not infringe third-party IP; and (f) processes dates, currencies (multi-currency incl. KES/USD), and Kenyan statutory requirements (tax, payroll) correctly, with statutory updates provided within maintenance.

5.2 Warranty period: for each Release, twelve (12) months from its Go-Live Declaration or six (6) months from Operational Acceptance, whichever is longer ("Software Warranty Period"), during which all non-conformities are corrected at the Contractor's cost, in addition to and not limited by SLA obligations.

5.3 Custom development warranty: custom objects (RICEFW), integrations and reports carry the same warranty and are additionally warranted to be delivered with source artefacts, deployment scripts, technical specifications and inline documentation to professional standards, maintainable by a competent third party.

5.4 SaaS warranty: SaaS Services will materially conform to their documentation and the contracted service descriptions continuously during the subscription term; the availability, security, residency and exit warranties of the SCC apply for the full term, not merely a warranty window.

SCHEDULE 6: HARDWARE WARRANTIES

6.1 All hardware (servers, storage, data protection appliances, network/load balancing components) is warranted: brand new and genuine from the OEM's authorised Kenya channel; current-GA and not EOL/EOS at delivery; serialised and registered to the KPC PLC on the OEM support portal; and conforming to the approved bill of materials and sizing specification.

6.2 OEM warranty and support: minimum **three (3) years, 24x7, OEM-backed, with Next Business Day on-site response in Kenya**, running from commissioning certificates (not shipment), covering parts, labour and firmware; extendable to years four (4) and five (5) at

rates fixed in the BOM. Mission-critical tiers (production storage, core compute) shall carry [4-hour] response uplift where specified in the BOM.

6.3 DOA and epidemic failure: units failing within thirty (30) days of installation are replaced new within fourteen (14) days. If ≥ [5]% of any product line fails within twelve (12) months, the Contractor shall implement an OEM-supported fleet remediation (firmware, batch replacement) at no cost.

6.4 Media retention: failed storage media containing KPC PLC data shall remain with the KPC PLC (keep-your-drive); replacement is provided without surrender of the failed media.

6.5 Spares and logistics: the Contractor shall maintain in-country critical spares (or OEM-committed spares logistics) sufficient to meet the SLA hardware resolution targets, evidenced at each service review.

SCHEDULE 7: RIGHTS TO USE (TENDERER TO PROVIDE ALTERNATIVE)

7.1 Licence grant: the KPC PLC receives, per product, the broadest of the OEM's standard enterprise grant and the following minimum rights: use by the KPC PLC, its subsidiaries and successor entities (including any restructured state successor), for the KPC PLC's business, by employees, contractors, secondees and authorised third parties acting for the KPC PLC, across all KPC PLC sites and the contracted user counts.

7.2 Included use rights without additional fee: production, DEV, TST, UAT, training and DR environments; disaster invocation and DR testing; backup and archival copies; read-only access for auditors and regulators; reasonable evaluation sandboxes; and API access within licensed capacity for integration and data extraction, including extraction for exit.

7.3 Outsourcing/operation by third parties: the KPC PLC may permit a successor support provider or outsourcer to operate the Solution on its behalf without additional licence fees, subject to confidentiality undertakings.

7.4 Term of rights: perpetual for perpetual licences; for subscriptions, for the paid term with the renewal protections of the SCC; custom deliverables vest in the KPC PLC outright; Contractor background IP is licensed perpetually and royalty-free for use with the Solution. Direct licence confirmations from the ERP OEM and E-Procurement Provider preserve these rights independent of the Contractor.

7.5 No use restriction shall prevent the KPC PLC processing data of its customers, partners and government counterparties within the Solution in the ordinary course of its business.

SCHEDULE 8: ACCEPTANCE FRAMEWORK AND TIMELINE (TENDERER TO PROVIDE ALTERNATIVE)

8.1 Acceptance is exclusively by the KPC PLC's written certificates per the stages below; productive use, partial use or lapse of time never constitutes deemed acceptance of a deliverable or Release. The KPC PLC's review of documentary deliverables follows a 10-business-day review / 5-business-day re-review cycle; review comments must be addressed in full before re-submission.

8.1A Acceptance Stages and Indicative Timeline (T0 = Effective Date)

#	Payment Milestone	Certifiable Milestone Outputs	Acceptance Gate
1.	Project Initiation	Project kickoff minutes; Project Charter; Implementation Plan; WBS; detailed schedule; governance framework; project team arrival; risk register; communication/change plan;	Gate 1 – Project Readiness: Project team mobilized; governance approved; project plan baselined; WBS and schedule approved; risks/dependencies registered; project controls operational; formal kickoff completed
2.	Infrastructure Delivery to the KPC Site – Inspected and Accepted	Packing lists; bills of landing or airway bills; certificates of origin; insurance certificates; serial number schedule; goods received note; inspection report confirming no damage and correct configuration against the BOM	Gate 2: Delivery Notes and Acceptance Certificates against the BOM
3.	Infrastructure Installation Integration & Acceptance: completion with site acceptance tests; passed Delivery of Full software licenses entitlements delivered and verified as installed in KPC's development and test environments.	As-built rack elevations and cabling schedules; power and cooling sign-off; firmware and patch baseline recorded; performance and failover test results against the technical specification; Operational Acceptance Certificate; capacity and performance report at production load. Entitlement certificates issued in the name of Kenya Pipeline Company PLC; licence portal and licence server access transferred to KPC; installation report countersigned by KPC ICT; reconciliation of licence metric and count against the BOQ	Gate 3 – Infrastructure Readiness: All contracted infrastructure installed/configured; connectivity validated; Dev/Test/UAT/Production environments operational; backup/restore tested; security hardening completed; performance/capacity tests passed; infrastructure ready to support solution implementation; Infrastructure Acceptance Certificate issued Gate4 - Install Software license: Operational Acceptance Certificate; production instance registered against KPC entitlements Final Acceptance Certificate; licence compliance report demonstrating entitlement equal to or greater than deployment and licence quantities reconciled with the BOQ
4.	Business & Technical Requirements Sign-off Solution Architecture	Completed As-Is Assessment; To-Be Processes; BRS; FRS; TRS; RTM; Gap Analysis; Data & Integration Requirements Solution Architecture;	Gate 5 – Requirements Baseline: 100% of agreed business areas/processes assessed; requirements documented and traceable; major gaps resolved/accepted; To-Be processes

	& Detailed Design Approval	Application, Data, Integration, Infrastructure & Security Architecture; Disaster Architecture; Detailed Design; Security Design	approved; requirements baseline formally signed off Gate 6 – Design Approval: Architecture compliant with approved requirements; security, integration, data and infrastructure designs approved; design review issues resolved; no outstanding critical design issues; Technical Design Authority approval issued
5.	Configuration, Development & Integration Completion	Configured modules; custom developments; APIs/interfaces; workflows; reports/dashboards; migration scripts; configuration documentation; SIT-ready solution Subscription to Saas deliverable MSOOS/TMS, OT integration and depot systems (five depots)	Gate 5 – Build Completion: Agreed functionality configured/developed; interfaces operational; unit testing completed; agreed defects within permitted threshold; RTM demonstrates coverage of requirements; solution technically ready for SIT; Build & Integration Completion Certificate issued
6.	System Integration Testing (SIT) Completion	SIT plan; test scripts; executed tests; integration results; performance/security testing; defect register; SIT report	Gate 6 – SIT Acceptance: Agreed SIT test cases executed; critical business/integration scenarios successfully passed; no unresolved Critical defects; High defects resolved or formally accepted with remediation plan; integrations validated; performance/security tests completed; SIT Acceptance Certificate issued Configuration workbooks; unit and integration test results; defect log; development, QA and pre-production environments handed over.
7.	UAT, Training & Operational Readiness	UAT plan/results; UAT sign-off; training programme; manuals; training records; SOPs; support procedures; operational readiness assessment Reconciliation report for every migrated object, signed by the named data owner; cleansing exception log closed.	Gate 7 – Business Readiness: UAT successfully completed; business owners sign off; Critical/High defects preventing business operation resolved; agreed users trained; support model operational; SOPs approved; business and operational readiness confirmed; UAT & Operational Readiness Certificate issued SAT passed, including the interface to the ERP; earned individually per depot site. Order-to-cash and terminal operations demonstrated end to end

			in production for a continuous 30-day period across all five depots.
8.	Production Deployment & Go-Live	Cutover Plan; Data Migration Report; Reconciliation Report; Production Deployment Report; Go-Live Checklist; production validation; support activation	Gate 8 – Production Acceptance: Cutover successfully completed; agreed data migrated and reconciled; production environment operational; critical business processes successfully validated; support/helpdesk operational; rollback/contingency arrangements confirmed; authorized Go-Live Certificate issued as agreed end-to-end transaction set processed in production.
9.	Hypercare & Stabilization Expiry of Defects Liability Period	Hypercare Report; SLA/KPI Report; Incident & Defect Report; Performance Report; Adoption Report; Stabilization Report; Knowledge Transfer Report	Gate 9 – Stabilization: System operating satisfactorily in production for agreed stabilization period; SLA/KPI thresholds achieved; no unresolved Critical defects; High defects within agreed tolerance; incident volumes stabilized; support team demonstrably capable; Stabilization Acceptance Certificate issued Expiry of Defects Liability Period-Certificate of expiry. 12 months from Operational Acceptance elapsed; all warranty defects closed or waived in writing by KPC.
10.	Final Acceptance, Handover & Knowledge Transfer	Final Acceptance Report; as-built architecture; technical documentation; configuration records; security/DR documents; O&M manuals; knowledge transfer; asset register; closure report	Gate 10 – Final Acceptance: All contractual deliverables accepted; documentation complete; knowledge transfer completed; outstanding defects within agreed warranty/support arrangements; assets and configurations handed over; support/warranty activated; project closure approved; Final Acceptance Certificate issued

8.2 Conditional acceptance: the KPC PLC may, at its sole discretion, certify a stage subject to a punch list of Severity 3/4 items with committed dates; punch items unresolved by their dates are treated as SLA breaches and withhold [10]% of the associated milestone payment until closure.

8.3 Rejection: where a stage fails, the Contractor bears the cost of re-work and re-test, and the Milestone LD regime of the SCC applies to the resulting delay. Two (2) consecutive

rejections of the same stage escalate to the Steering Committee with a recovery plan requirement.

SCHEDULE 9: QUALITY MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE)

9.1 The Contractor shall operate the engagement under its ISO 9001-certified QMS and deliver, within thirty (30) days of T0, a Programme Quality Plan for KPC PLC approval covering: deliverable standards and templates; review and approval workflows; configuration and release management (all changes via version-controlled transport/pipeline with segregation of duties — no direct changes in production); document management in the programme repository; internal quality gates preceding every KPC PLC submission; measurement (first-time-acceptance rate, defect density, rework); and audit arrangements.

9.2 Quality gates: each Release passes internal Contractor quality gates (design complete, build complete, test readiness, go-live readiness) evidenced by signed gate checklists before the corresponding KPC PLC stage review. The PMO may audit gate evidence and attend gate reviews.

9.3 Audits: the KPC PLC and PMO may conduct quality audits on fourteen (14) days' notice (unannounced for site HSE); nonconformities are remediated per an agreed corrective action plan; repeated major nonconformities escalate to the Steering Committee and count against the Contractor's performance assessment under PPADA contract management requirements.

9.4 First-time-acceptance rate of documentary deliverables below [80]% in any quarter triggers a quality improvement plan at the Contractor's cost, including senior QA reinforcement.

SCHEDULE 10: GO-LIVE MANAGEMENT (TENDERER TO PROVIDE ALTERNATIVE)

10.1 Go-Live Readiness Criteria (per Release/Wave)

10.1.1 The Go/No-Go review shall verify, as minimum criteria: all Schedule 1 stage certificates issued; migration reconciliation certificate signed (Schedule 2.3.1); cutover runbook rehearsed within the approved window with contingency headroom of ≥ [30]%; rollback plan tested; support model staffed (service desk, Hypercare roster, OEM standby); business readiness confirmed by the Change workstream (training completion ≥ [90]% of target users, SOPs published); security sign-off (pen test findings closed, SoD validated, IAM provisioning complete); OT MOC approvals in place for affected sites; interfaces to banks/KRA certified in partner test environments; and legacy freeze and dual-running plan approved.

10.2 Go/No-Go Governance

10.2.1 The Go/No-Go decision is made by the Steering Committee (or its delegated authority) on a written readiness report jointly presented by the Contractor and PMO not less than five (5) business days before the planned cutover. Checkpoint go/no-go decisions during cutover

execution rest with the KPC PLC's Cutover Manager. A No-Go for Contractor-attributable reasons re-schedules cutover at the Contractor's cost; the Milestone LD regime applies.

10.3 Cutover Execution

10.3.1 Cutover executes per the rehearsed runbook (task-level owners, timings, checkpoints), within the KPC PLC-approved window selected to avoid month-end close, payroll runs and peak loading days; TMS/depot waves cut over depot-by-depot with the pilot depot stabilised for [2] weeks before subsequent waves. Overrun LDs and rollback obligations apply per the SCC.

10.4 Hypercare

10.4.1 Hypercare (90 days per Release) provides: on-site functional and technical floor-walkers at head office and pilot sites; daily defect triage with the KPC PLC and PMO; twice-weekly stabilisation reporting (incident trends, backlog, business KPIs such as invoice cycle time, loading throughput, payroll accuracy); and immediate root-cause analysis for any Severity 1. Hypercare exit criteria: two (2) consecutive weeks with zero Severity 1, Severity 2 within SLA, incident arrival trending down, all business-critical KPIs at or above pre-cutover baseline, and knowledge transfer for first-line support completed. Hypercare extends at the Contractor's cost until exit criteria are met.

SCHEDULE 11: DEFECT LIABILITY AND SUPPORT PERIOD (TENDERER TO PROVIDE ALTERNATIVE)

11.1 Structure of post-implementation cover: (a) Hypercare per Schedule 10.4; (b) Software Warranty Period per Schedule 5.2 and hardware warranty per Schedule 6 (together the "Defect Liability Period"); and (c) the [36]-month Support Term under the SLA from Operational Acceptance, with per-Release interim support from each Go-Live. These operate concurrently; warranty corrections are never chargeable and never consume KPC PLC support entitlements.

11.2 During the Defect Liability Period the Contractor shall correct, at its cost: functional non-conformities against the Requirements Baseline; performance shortfalls against Clause 16 benchmarks; migration-attributable data defects (12 months per Schedule 2.3.2); custom-object failures including those triggered by OEM patches; and configuration errors, in each case including consequential data repair.

11.3 Retention of [10] % of the implementation price is held until six (6) months after final Go-Live (releasable earlier against an on-demand bank guarantee of equal value), securing Defect Liability Period performance in addition to the Performance Security.

11.4 At the end of the Support Term the KPC PLC holds pre-priced options to extend support for two (2) further periods of twelve (12) months at the capped escalation rates in the SCC, and the exit assistance obligations of the SCC apply.

SCHEDULE 12: MILESTONE SIGN-OFF MATRIX (TENDERER TO PROVIDE ALTERNATIVE)

12.1 Every milestone is closed only by a written certificate in the form annexed to the Contract, signed by the certifiers below, supported by the listed evidence, and recorded in the programme repository by the PMO. Certificates state any punch list and payment consequence. The matrix below is the single authoritative sign-off scheme:

Milestone	Contractor Signatory	KPC PLC Certifier(s)	Assurance / Witness

12.2 Certificates require signature within ten (10) business days of the KPC PLC being satisfied the criteria are met; the KPC PLC's reasons accompany any refusal so the Contractor can remediate. No certificate is valid if procured by misrepresentation, and certification does not waive latent defects, the Solution Standards warranties, or the KPC PLC's audit rights.

12.3 A consolidated Sign-Off Register (milestone, certificate reference, date, signatories, punch list status, payment linkage) is maintained by the PMO and tabled at every Steering Committee; it is the definitive record for payment certification under the SCC and for PPADA contract management reporting.

SECTION VI-A: SERVICE LEVEL AGREEMENT (SLA) SCHEDULE

This SLA Schedule forms part of the Contract and defines the minimum service performance obligations. The Vendor shall meet or exceed all SLA targets from the Go-Live Date (or from the date specified in the SCC).

A. SLA TARGETS AND RESPONSE TIMES

Priority	Definition	Acknowledge	Resolve	Service Credit (% of Monthly Fee)

P1 — Critical	System completely unavailable; business operations halted; security breach	15 minutes	4 hours	5% per hour of breach (max 50% monthly)
P2 — High	Major functionality unavailable; significant business impact; no workaround	30 minutes	8 hours	2% per hour of breach (max 20% monthly)
P3 — Medium	Partial functionality affected; workaround available; moderate impact	2 hours	24 hours	1% per incident (max 10% monthly)
P4 — Low	Minor issue; minimal impact; service request	4 hours	5 business days	No credit; escalate if persistent
P5 — Change	Enhancement or change request — planned; no urgency	1 business day	Per agreed change schedule	Not applicable

B. SYSTEM AVAILABILITY AND UPTIME TARGETS

System / Service	Target Uptime	Measurement Period	Maximum Planned Downtime
Mission-Critical Systems (SCADA, Pipeline Mgt, Core ERP)	99.5%	Monthly (excluding planned maintenance)	4 hours per month; off-peak only
Operational Systems (HR, Finance, BI, CRM)	99.0%	Monthly	8 hours per month; weekends preferred
Standard Systems (Email, Office, Collaboration)	99.0%	Monthly	8 hours per month
SaaS / Cloud Services	Per vendor SLA (minimum 99.5% for mission-critical)	Monthly	As per vendor maintenance schedule

C. PATCH MANAGEMENT AND SECURITY UPDATE TARGETS

Patch Severity	Deployment Target	Verification

Critical Security Patches	Within 48 hours of vendor release; emergency change procedure	Patch report to KPC PLC IT within 24 hours of deployment
High Severity Patches	Within 7 calendar days of release	Monthly patch compliance report
Medium Severity Patches	Within 30 calendar days	Monthly patch compliance report
Low / Informational	Within 90 calendar days or at next scheduled maintenance	Quarterly patch summary
Operating System / Platform Upgrades	As agreed in advance change schedule	Change approval documentation

D. BACKUP, RECOVERY AND BUSINESS CONTINUITY

Backup Frequency	Daily incremental backup; weekly full backup
Backup Retention	Daily: 30 days; Weekly: 12 months; Monthly: 7 years (regulatory)
Backup Testing	Monthly restore test; results reported to KPC PLC
Recovery Time Objective (RTO)	4 hours for mission-critical systems; 8 hours for operational systems
Recovery Point Objective (RPO)	Maximum 24 hours for all systems; 4 hours for mission-critical
Disaster Recovery Site	[Vendor-provided / KPC PLC DR site — specify location]
DR Test Frequency	Annual DR drill; report to KPC PLC IT within 30 days
BCP Documentation	Vendor to provide BCP/DRP document aligned to this SLA within 60 days of Go-Live

E. REPORTING OBLIGATIONS

Report	Frequency	Due Date
Monthly SLA Performance Report	Monthly	Within 5 working days after month-end

Security / Vulnerability Report	Monthly	Within 5 working days after month-end
Patch Compliance Report	Monthly	Within 5 working days after month-end
Incident Root Cause Analysis (P1/P2)	Per major incident	Within 5 working days of incident resolution
Capacity and Performance Report	Quarterly	Within 10 working days after quarter-end
Licence Usage Report	Quarterly	Within 10 working days after quarter-end
Annual Security Penetration Test Report	Annual	Within 30 days of test completion
DR Test Report	Annual	Within 30 days of DR test

PART 6 – CONTRACT FORMS AND SCHEDULES

SECTION VII: CONTRACT FORMS

FORM C1: CONTRACT AGREEMENT

THIS CONTRACT AGREEMENT is entered into on the _____ day of _____ 20___ by and between:

(1) KENYA PIPELINE COMPANY PLC, incorporated under the Companies Act 2015, with registered office at Kenpipe Plaza, Sekondi Road, Off Nanyuki Road, Industrial Area, P.O. Box 73442-00100, Nairobi, Kenya ('KPC PLC'); and

(2) [NAME OF VENDOR], incorporated under the laws of [Country], with offices at [Address] ('the Vendor').

WHEREAS KPC PLC issued Tender Reference No. _____ for [Project Title] and accepted the Vendor's Tender dated _____ following evaluation and negotiations:

IT IS AGREED that the Vendor shall supply [describe scope] in accordance with the Contract Documents.

Contract Price: KES _____ (Year 1) | TCO over [___] years: KES _____

Commencement Date: _____ | Target Go-Live Date: _____

Contract Documents (in order of priority): Contract Agreement → Change Requests → SCC → SLA Schedule → GCC-IT → Technical Specifications/Terms of Reference → BOM → Vendor's Technical Proposal.

KPC PLC: Signature _____ Name _____ Title _____ Date _____ Seal _____

Vendor: Signature _____ Name _____ Title _____ Date _____ Seal _____

FORM C2: PERFORMANCE SECURITY (BANK GUARANTEE)

[Letterhead of Bank] | To: Kenya Pipeline Company PLC

WHEREAS [Vendor] has entered into IT Contract No. _____ with KPC PLC for [Project Title], WE [Bank Name], a bank licensed by the CBK, irrevocably guarantee to pay KPC PLC on first written demand, without cavil or argument, any sum up to KES _____, in the event that the Vendor fails to perform its obligations under the Contract.

Valid until: _____ [Contract Period + 90 days after FAC]

Bank Signature: ____ Stamp: ____ Date: ____

FORM C3: PROVISIONAL ACCEPTANCE CERTIFICATE (PAC)

PAC No.	PAC-[Number]
Contract Reference	
Vendor	
System / Project	
UAT Completed	Yes / Pending [specify]
SIT Completed	Yes / Pending [specify]
Performance Test	Passed / Pending [specify]
Security Test	Passed / Deferred [specify]
Open Issues (P1/P2)	[None / List]
Training Completed	Yes / Scheduled [date]
Documentation Received	Yes / Pending [specify]
Warranty Start Date	
Hypercare Period	From: ___ To: ___ ([days] days)
PAC Status	GRANTED / NOT GRANTED (see conditions below)
Conditions (if any)	

Approvals

	Name	Signature	Date
Functional/Technical Team Lead			
PMO External			

PMO Internal			
BPO			
GM BPO			
IT Director			

FORM C4: FINAL ACCEPTANCE CERTIFICATE (FAC)

This Certificate confirms that [Vendor] has satisfactorily completed all obligations under Contract No. _____ for [Project Title].

All P1/P2 bugs resolved: ____ All Deliverables accepted: ____ Training completed: ____

Documentation (technical/user manuals) received: ____ Knowledge transfer complete: ____

Escrow deposit confirmed (where applicable): ____ IP assignment completed: ____

Performance Security: Released — return within 30 days of this FAC.

Warranty Period: From ___ to ___ Support/SLA Period commences: ___

Total Amount Paid: KES ___ Outstanding: ___

KPC PLC: Signature ____ IT Director ____ GM Supply Chain ____ Date ____

FORM C5: CHANGE REQUEST AND CHANGE ORDER

Change Request No. ____ Contract No. ____ Date: ____

Requested By (KPC PLC): ____ Received By (Vendor): ____

Description of Change Requested	
Business Justification	
Vendor's Impact Assessment — Scope	
Vendor's Impact Assessment — Contract Price	[Increase KES ___ / Decrease KES ___ / No Change]
Vendor's Impact Assessment — Timeline	[Extension ___ days / No Change]
Vendor's Impact Assessment — SLA	[Change required / No Change]
Vendor's Impact Assessment — Security	[Security review required / No Change]
KPC PLC Decision	[Approved / Rejected / Deferred] — Date: ___

Revised Contract Price (if approved)	KES ___
Revised Go-Live / Milestone (if approved)	

KPC PLC Authorised: ____ Vendor Authorised: ____ Date: ____

APPENDIX A — TECHNICAL SPECIFICATIONS/TERMS OF REFERENCE AND PROJECT CHARTER

[To be completed for each IT project. Shall include:]

- Project background, business objectives and success criteria
- Functional requirements — what the system must do
- Technical requirements — infrastructure, performance, integration, security standards
- Non-functional requirements — availability, scalability, response time, concurrent users
- Interface and integration requirements — systems to be integrated, APIs, data exchange formats
- Data migration requirements — source systems, data volumes, transformation rules, validation criteria
- Security requirements — authentication, authorisation, audit trail, encryption, compliance standards
- Compliance requirements — industry regulations, KPC PLC internal standards
- KPC PLC's existing IT environment description (to enable integration assessment)
- Future scalability requirements — anticipated growth over 5 years
- Exclusions — what is specifically out of scope

APPENDIX B — BILL OF MATERIALS (BOM)

[Completed version from Form FP-IT-2 — incorporated into Contract Agreement at award]

APPENDIX C — APPROVED KEY PERSONNEL

No.	Name	Role	Certifications	Commitment (%)
1				
2				
3				
4				

APPENDIX D — IMPLEMENTATION PLAN (BASELINE)

[Agreed Implementation Plan (from Form TP-IT-5, as modified during negotiations) — incorporated into Contract at award. Any subsequent revision requires a Change Request.]

ANNEXURES

ANNEXURE A: GLOSSARY OF KEY TERMS

Term	Meaning
AES-256	Advanced Encryption Standard — 256-bit key length; current gold standard for data encryption at rest
AMC	Annual Maintenance Contract — 12-month support and maintenance agreement
ATG	Automatic Tank Gauging
BCP	Business Continuity Plan — plan to maintain operations during disruptions
BOM	Bill of Materials — itemised list of all hardware, software and licences with quantities and prices
CBK	Central Bank of Kenya
CMDB	Configuration Management Database — inventory of all IT assets and their relationships
COTS	Commercial Off-The-Shelf — standard, mass-market software product
DR	Disaster Recovery — procedures to restore IT systems after a disruptive event
EoL	End of Life — date after which a product receives no vendor security patches or support
ERP	Enterprise Resource Planning — integrated business management software (e.g., SAP)
FAC	Final Acceptance Certificate — confirms successful completion of all contract obligations
FAT	Factory Acceptance Test — testing at Vendor's premises before delivery
GDPR	General Data Protection Regulation (EU) — may apply where EU personal data is involved
GCC-IT	General Conditions of Contract for IT Procurement (Section V of this STD)
HA	High Availability — system design ensuring minimal downtime through redundancy
IaaS	Infrastructure as a Service — cloud-based computing infrastructure
ISMS	Information Security Management System — framework for managing information security
ITIL	Information Technology Infrastructure Library — framework for IT service management
KES	Kenya Shillings

KPC PLC	Kenya Pipeline Company PLC
MFA	Multi-Factor Authentication — requiring two or more verification methods for system access
MM	Material Management
MSP	Managed Service Provider — company providing outsourced IT management services
MTTR	Mean Time to Repair — average time to restore a failed system or component
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NOC	Network Operations Centre — centralised facility for monitoring IT infrastructure
OEM	Original Equipment Manufacturer — primary manufacturer of hardware or software
OMC	Oil Marketing Companies
OWASP	Open Web Application Security Project — community for web application security standards
PaaS	Platform as a Service — cloud-based platform for developing and deploying applications
PAC	Provisional Acceptance Certificate — confirms Go-Live readiness after UAT
PMP	Project Management Professional — PMI certification for project managers
PoC	Proof of Concept — demonstration to validate proposed solution
PEKL	Konza Depot
PS01	Mombasa Depot
PS02	Samburu Pump Station
PS03	Maungu Pump Station
PS04	Manyani Pump Station
PS05	Mtito Andei Pump Station
PS06	Makindu Pump Station
PS07	Sultan Hamud Pump Station
PS08	Konza Pump Station
PS09	Embakasi Aviation Depot
PS10	Nairobi Terminal Depot
PS11	Nairobi Terminal Transfer

PS12	Moi Airport Depot
PS14	Kipevu Oil Storage Facility
PS15	Kenya Petroleum Refineries Ltd
PS21	Nairobi Terminal Pump Station
PS22	Ngema Pump Station
PS23	Morendat Pump Station
PS24	Nakuru Pump Station
PS25	Nakuru Depot
PS26	Sinendet Pump Station
PS27	Eldoret Depot
PS28	PS28 Kisumu Depot
RBAC	Role-Based Access Control — access permissions assigned based on user roles
RPO	Recovery Point Objective — maximum acceptable data loss measured in time
RTO	Recovery Time Objective — maximum acceptable time to restore IT services
RTM	Requirements Traceability Matrix
SaaS	Software as a Service — software accessed via the internet on subscription basis
SAT	Site Acceptance Test — testing at KPC PLC's site after delivery and installation
SBOM	Software Bill of Materials — complete list of software components and their licences
SCADA	Supervisory Control and Data Acquisition — industrial control system software
SCC	Special Conditions of Contract
SIEM	Security Information and Event Management — real-time security monitoring
SIT	System Integration Test — verifying the system works with connected systems
SLA	Service Level Agreement — contractual performance obligations and remedies
SOC 2	Service Organization Control 2 — auditing standard for service providers handling data
SRM	Supplier Relationship Management (SAP module)

STD	Standard Tender Document
TCO	Total Cost of Ownership — comprehensive financial evaluation over the system lifecycle
TDS	Tender Data Sheet
TLS	Transport Layer Security — protocol for encrypting data in transit (minimum TLS 1.2)
UAT	User Acceptance Test — testing by KPC PLC end-users to confirm system meets needs
VAR	Value-Added Reseller — company that resells products with added services
VPN	Virtual Private Network — encrypted connection for secure remote access

ANNEXURE B: KPC PLC ETHICS POLICY SUMMARY

- Fair Competition: KPC PLC ensures a level playing field. All Tenderers receive the same information and access.
- Anti-Corruption: Zero tolerance for bribery, kickbacks, or corrupt influence. Ethics Hotline: report.fraud@kpc.co.ke.
- Conflict of Interest: All conflicts must be disclosed. Firms involved in specifications preparation are disqualified.
- Confidentiality: Tender documents and evaluation proceedings are confidential until award.
- Intellectual Property: KPC PLC respects vendors' IP and requires vendors to respect third-party IP.
- Sustainability: KPC PLC encourages vendors to demonstrate environmental sustainability in IT procurement (energy efficiency, e-waste management, circular economy principles).

ANNEXURE C: CYBERSECURITY REQUIREMENTS FOR IT VENDORS

All IT vendors providing systems or services that connect to, process or store KPC PLC data shall comply with the following minimum requirements:

C.1 Information Security Management

- Maintain an Information Security Management System (ISMS) aligned with ISO/IEC 27001 or demonstrate equivalent controls;
- Provide an executive-level Information Security Officer (CISO or equivalent) as the point of contact for security matters;
- Conduct annual security awareness training for all staff with access to KPC PLC systems.

C.2 Access and Identity Management

- Implement Role-Based Access Control (RBAC) for all KPC PLC system access;

- Enforce Multi-Factor Authentication (MFA) for all privileged/administrative accounts;
- Implement the principle of least privilege — access granted only as required for the role;
- Log and monitor all privileged access; provide access logs to KPC PLC on request.

C.3 Data Security

- Encrypt all KPC PLC data at rest using AES-256 or equivalent;
- Encrypt all data in transit using TLS 1.2 or higher;
- Implement data loss prevention (DLP) controls where relevant;
- Maintain data residency in Kenya unless KPC PLC provides explicit written consent for offshore processing.

C.4 Vulnerability and Patch Management

- Conduct automated vulnerability scanning of all systems at least monthly;
- Conduct annual penetration testing by an independent CREST/OSCP-certified tester;
- Deploy critical security patches within 48 hours; high within 7 days; medium within 30 days;
- Maintain a complete, current Software Bill of Materials (SBOM) for all software components.

C.5 Incident Response

- Maintain a documented Incident Response Plan (IRP) tested at least annually;
- Notify KPC PLC of any security incident affecting KPC PLC systems or data within 4 hours;
- Provide a preliminary incident report within 24 hours and a full root cause analysis within 5 business days;
- Cooperate with KPC PLC in any forensic investigation.

C.6 Supply Chain Security

- Disclose all third-party software components (SBOM);
- Ensure all subcontractors with access to KPC PLC systems are subject to equivalent security obligations;
- Hardware: provide evidence that components are sourced through authorised channels (no counterfeit components).

ANNEXURE D: DATA PROTECTION REQUIREMENTS

Where IT Vendors process KPC PLC personal data, the following requirements apply under the Data Protection Act 2019:

- A formal Data Processing Agreement (DPA) shall be executed before any personal data access;
- Processing is limited to the minimum data necessary for the IT project ('data minimisation');

- Vendor shall maintain a Record of Processing Activities and make it available to KPC PLC on request;
- Data breach notification: within 24 hours of discovery to KPC PLC; within 72 hours to ODPC if required;
- Vendor shall appoint a Data Protection Officer (DPO) where required by law;
- Data subject rights: Vendor shall assist KPC PLC in responding to access, rectification, erasure and portability requests;
- Cross-border transfers: only with KPC PLC's written consent and adequate safeguards;
- Data destruction: all KPC PLC data to be securely destroyed at contract end; certificate of destruction provided;
- KPC PLC Data Protection Officer: xxx@kpc.co.ke

ANNEXURE E: TENDERER SUBMISSION CHECKLIST

No.	Item	Included? (Y, N, N/A)
1	Form TP-IT-1: Technical Proposal Submission Form — signed	
2	Form TP-IT-2: Tenderer Profile, Credentials and Project Experience — completed	
3	Form TP-IT-3: Technical Solution Description — with architecture diagram	
4	Form TP-IT-4: Technical Compliance Matrix — completed for ALL requirements	
5	Form TP-IT-5: Implementation Plan — with Gantt chart	
6	Form TP-IT-6: Proposed Team — with signed CVs for all Key Personnel	
7	Form TP-IT-7: SLA Proposal — with specific SLA parameter commitments	
8	Form TP-IT-8: Cybersecurity and Data Protection Declaration — signed	
9	Form OEM-IT: OEM Authorisation Letters — for all specified brands (current and verified)	
10	Form COI-IT: Conflict of Interest Declaration — signed	
11	Form BOD-IT: Beneficial Ownership Disclosure — completed	
12	Form ACD-IT: Anti-Corruption Declaration — signed	
13	Tender Security — correct form and amount (where required by Data Sheet)	
14	Valid KRA Tax Compliance Certificate (Kenyan firms)	

No.	Item	Included? (Y, N, N/A)
15	Certificate of Incorporation / Business Registration	
16	ICT Authority Registration (where required)	
17	ISO/IEC 27001 Certificate or equivalent cybersecurity certification (current)	
18	SOC 2 Type II Report (for cloud/managed services — issued within last 12 months)	
19	Audited Financial Statements (last 3 years)	
20	Client References for at least 3 relevant IT projects (contact details for referees)	
21	TECHNICAL PROPOSAL CONTAINS NO FINANCIAL OR COST INFORMATION	
22	FINANCIAL PROPOSAL (Forms FP-IT-1 to FP-IT-2) submitted SEPARATELY in SAP SRM Financial Proposal workspace (or sealed envelope where applicable)	

ANNEXURE F: CONTACT INFORMATION

Procurement Contact	General Manager — Supply Chain, KPC PLC
Physical Address	Kenpipe Plaza, Sekondi Road, Off Nanyuki Road, Industrial Area, Nairobi
Postal Address	P.O. Box 73442-00100, Nairobi, Kenya
Website	www.kpc.co.ke
Procurement Email	opentender@kpc.co.ke
Ethics / Fraud Hotline	
Data Protection Officer	
IT Department (Technical Queries)	
SAP SRM Portal (Tender Submission)	
~~**NCIA (Dispute Resolution)**~~	~~www.ncia.or.ke~~
KRA (Tax Compliance Verification)	www.kra.go.ke
ICT Authority Kenya	www.ict.go.ke

Kenya Data Protection Act — ODPC	www.odpc.go.ke