THE DIGITAL MALAWI ACCELERATION PROJECT

GRANT NUMBER : IDA-E338-MW

PROJECT NUMBER : P505095

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES TO MIGRATE GOVERNMENT DATA TO THE NATIONAL DATA CENTRE

CONTRACT NO: MW-PPPC-450230-CS-CQS

DATE: JANUARY 2025

A. BACKGROUND

The Government of Malawi, through the Ministry of Information and Digitalization and the Department of e-Government, has established a National Data Centre in Lilongwe that will be used for hosting the majority of critical government systems, applications and data. The National Data Centre aims at harmonizing Government-wide systems in one modern place that is has high availability, reliable energy source, secure and with reliable connectivity. This brand-new facility,is envisioned to provide shared access to applications and data using a complex network, computing, and storage infrastructure. The new data centre will be running off Nutanix Hyperconverged Infrastructure (HCI) as a modern IT architecture that consolidates compute, storage, and networking into a single software-defined platform. Nutanix offers a solution that simplifies data centre management and scales seamlessly to meet the demands of businesses of all sizes. Some of the key components include:

i) Software-Defined Architecture: Nutanix HCI replaces traditional hardware-based infrastructure with a software-driven model, enabling agility and cost efficiency. For compute, it virtualizes workloads using a hypervisor. For storage, it provides distributed and software-defined storage. And for networking, it Integrates virtual networking for seamless connectivity and automated configuration.
ii) Nutanix offers flexibility with its native hypervisor, Acropolis Hypervisor, which also supports third-party hypervisors like VMware and Hyper-V.
iii) Nutanix has a centralized management interface, Prism, that simplifies monitoring, troubleshooting, and managing the infrastructure. Prism also automates routine tasks like patching and scaling.
iv) Nutanix HCI operates on a scale-out architecture, allowing organizations to start small and grow by adding nodes without disrupting operations.
v) Nutanix uses distributed redundancy, ensuring data protection and availability even if hardware fails due to integrated backup, disaster recovery, and robust data encryption that ensures business continuity.

The data centre will have 277.2 GHz of processing power, 2.63TB of memory and 107.52 of hard disk space. The facility is expected to become fully operational in March 2025 and will have 13 empty server racks that will be available for co-location.

The National Data Centre in Lilongwe will be the primary site and the Data Centre in Blantyre will be the disaster recovery (DR) site. This DR site will have identical server equipment as the primary site to allow seamless data replication that will facilitate data recovery and business continuity in the event of an outage of the primary site.

Presently, Government Ministries, Departments, and Agencies (MDAs) host their IT systems and applications in silos, in multiple server rooms around the country. There is now a need to migrate the priority systems of individual MDA to the National Data Centre and also plan for proper data backup and recovery.

These terms of reference outline the scope, objectives, methodology, deliverables, and timeline for the migration of government data into the National Data Centre and ensuring its proper back up. The migration aims to transfer applications, systems and

data from current storage systems to the National Data Centre infrastructure, ensuring improved data management, back up, security, and accessibility.

B. OBJECTIVE

The Department of e-Government intends to use services of a competent and qualified Consultant (firm) in the process of migrating data from the various MDAs to its newly commissioned National Data Centre. The role of the Consultant will be to provide strategic, organizational, and technical support to the government during the data migration to the National Data Centre.

The National Data Centre is located in Area 4, Lilongwe next to the Department of e-Government office premises. This facility will be the primary site and the disaster recovery / secondary / backup site will be the Data Centre that is located in Mandala, Blantyre.

The primary objectives of this data migration assignment are:

- To ensure a seamless transfer of all relevant data to the new national data centre.
- To enhance data security, availability, and management of government data.
- To minimize downtime and disruptions during the data migration process.
- To maintain data integrity and accuracy throughout the migration.
- To ensure compliance with relevant data protection and privacy regulations.

The scope of services, consulting team profiles, reporting requirements and other particulars of the assignment are detailed below.

C. SCOPE OF WORK

The consulting firm ("Consultant") will be expected to carry out the following tasks:

- Detailed assessments of the data currently hosted in multiple server rooms, data classification, and development of a comprehensive migration roadmap aligned with the government's goals.
- Management of the project timeline, coordination between ministries, and compliance with regulations and standards.
- Selection of migration tools ensuring the right technologies are used.
- Identification and mitigation of security, compliance, and operational risks throughout the migration process.
- Migration of data including but not limited to user data, transactional data, and historical data.
- Implementation of data security measures and data encryption.
- Validation and testing of the migrated data.
- Documentation, training and support for end-users post-migration.

The detailed scope of these works are as follows:

1. Assessment and Planning:

- Detailed assessment of the current data servers, focusing on hardware, software, data classification, and current security vulnerabilities at the targeted MDAs (please see Annex 1 for a list).
- Estimate data hosting capacity needed to host all of governments systems in the new datacentre. This information will be used to develop technical specifications for procurement of additional server infrastructure of the new datacentre.
- Ensure that all government data currently hosted at various MDAs is properly categorized (e.g., sensitive, confidential, or public).
- Prioritize what systems are to be migrated based on criteria and the 15 applications that will be agreed with the Department of e-Government.
- Identify gaps in security, performance, and compliance on the old systems in order to create a clear migration roadmap and address any immediate security concerns.
- Ensure that the migration complies with any national data protection regulations and international standards such as ISO 27001.
- Obtain a sign-off from the MDAs to validate the assessment results

2. Design a Secure Architecture:
   - Before any migration, ensure that all sensitive data is encrypted both at rest and in transit . Use robust encryption algorithms such as AES-256.
   - Isolate the data migration traffic from other network activities to prevent unauthorized access during the transfer.
   - Ensure that only authorized personnel have access to the data migration process.
   - Implement multi-factor authentication (MFA) for all systems involved.

3. Data Mapping and Design:
   - Define mapping rules between current storage systems and the new national data centre infrastructure.
   - Design migration scripts and tools.
   - Set up the target data centre environment.
   - Perform necessary network configurations.
   - Backup data and keep copies on-site and offsite.
   - Ensure disaster recovery plans are in place.

4. Data Cleansing and Optimization:
   - Eliminate redundant, obsolete, or trivial data from the old servers to reduce the migration load and focus resources on securing the most critical data.
   - Implement a comprehensive backup strategy. Take full backups before the data migration process begins and store them securely offsite (or in a cloud environment) in case data will need to be restored.

5. Develop a Detailed Migration Plan:
    - Plan the migration in phases, starting with non-critical systems before migrating sensitive or mission-critical data.
    - Set up a secure testing environment in the Data Centre that mirrors the actual environment. Perform dry-run migrations to identify issues before full-scale migration.
    - Ensure there is minimal impact on the day-to-day operations of ministries. Schedule migrations during off-peak hours and communicate downtime well in advance.

6. Amendments to the Migration Plan:
    - Assess the change to understand the reason for the change, identify impact that the change will bring, and prioritize the proposed changes.
    - Communicate with stakeholders to inform them the changes and their potential impact, and obtain feedback from then stakeholders on how the change may affect their areas.
    - Update the migration plan where necessary by adjusting the timeline, modifying the scope and reallocating resources.
    - Re-evaluate risks to identify any new risks introduced by the change, and develop strategies to mitigate those risks.
    - Test the adjustments by running simulations and validating data integrity, quality and accuracy.
    - Maintain detailed records of all changes, including the reason for the change, decisions made, and approvals received.
    - Obtain formal sign-off on the revised migration plan from Government department focal point and key stakeholders and project managers to ensure alignment.
    - Closely monitor the migration process to ensure the changes are properly implemented and provide stakeholders with frequent updates on the progress, especially if any issues arise.

7. Data Migration Tools and Techniques:
    - Use secure, industry-standard tools (such as Azure Migrate, AWS Server Migration Service, or VMware vMotion) for the migration process.
    - Use checksum or hash-based validation to ensure that data integrity is maintained during migration. Any discrepancies should be flagged and corrected immediately.
    - Use a VPN or Direct Connection: For data transfers, use secure VPN tunnels or direct fibre connections between the ministries and the Data Centre to avoid exposure to external threats.

8. Data Extraction:
    - Extract data from current storage systems according to the predefined mapping rules.

9. Data Transformation and Loading:
    - Transform data to fit the schema and storage requirements of the new data centre.
    - Execute data transfer using the chosen tools.
    - Load transformed data into the new server equipment in the national data centre.
    - Migrate applications, databases, and virtual machines.
    - Continuously monitor the migration process for issues.

10. Training:
    - Conduct training for ten (10) Department of e-Government staff members in data migration and application & system data backup.
    - Provide electronic copies of training materials for training participants.

11. Testing and Validation:
    - Conduct thorough testing and security audits to ensure data integrity and completeness.
    - Validate the migrated data against the original data.
    - Ensure application functionality.
    - Securely wipe the data from the old servers using industry-standard data wiping tools to prevent unauthorized recovery of sensitive information.
    - Monitor system performance and security.

12. Go-Live and Optimization:
    - Execute the final migration.
    - Switch operations to the new data centre.
    - Optimize performance and make necessary adjustments.
    - Document the entire migration process for future reference.

13. Post-Migration Support:
    - Provide support to address any post-migration issues.
    - Monitor the new environment, with real-time security alerts, logs, and reports, to ensure stability and any abnormal activity post-migration.
    - Conduct a post-migration review to identify lessons learned and areas for improvement.
    - Identify gaps in hosting capacity and assist in the development of technical specifications of the server equipment that may be required to accommodate the current and future data hosting needs of the entire government.

D. EXPECTED DELIVERABLES

The Consultant is expected to submit the following deliverables:

- **Inception Report**: Document that outlines the initial plans, objectives, and approach detailing how the assignment will be delivered.
- **Project Plan:** Detailed project plan outlining timelines, resources, and milestones.
- **MDA Data assessment Document:** Documentation of the current infrastructure at MDAs, current data structures and any dependencies.
- **Summary report on data hosting requirements if all of the systems are to be migrated to national datacenter**
- **Data Mapping Document:** Documentation of the data mapping rules and transformation logic.
- **Data Extraction Plan:** Detailed plan outlining how data will be extracted from current storage systems, how it will be backed up and transferred according to the predefined mapping rules.
- **Migration Scripts/Tools:** Developed scripts/tools for data extraction, transformation, and loading. At the minimum, the following tools to be used:
    - Planning and Assessment Tools
    - Data Migration Tools
    - Database Migration Tools
    - Virtual Machine Migration Tools
    - Storage Migration Tools
    - Network Configuration and Monitoring Tools
    - Security Tools
    - Validation and Testing Tools
    - Documentation and Collaboration Tools
- **Data Loading Plan:** Detailed plan outlining how data will be transferred from the current storage location using the chosen tools and how the transformed data will be loaded into the new server equipment in the national data centre. The plan should also show how applications, databases, and virtual machines will be migrated.
- **Testing Plan and Reports:** Detailed plan outlining how the migrated data will be for tested and presentation of reports of the results.
- **Security Plan:** Documentation of data security measures to be implemented.
- **Cutover Plan:** Detailed plan outlining how the final migration will be executed for Go-Live and how operations will be switched to the data centre.
- **Final Migration Report**: Comprehensive documentation of the entire migration process
- **User Training Materials**: Documentation and training materials for end-users.
- **Post-Migration Support Plan**: Plan for addressing post-migration issues and support.

E. SCHEDULE OF COMPLETION

The Consultant is expected to complete the assignment in full within twelve (12)

calendar months with an estimated level of input of 660-man days for key experts. The indicative timelines and payment schedule detailed below:

S/No	Milestone/deliverable	Timeline	Payment Schedule
1	Submission of Inception report and Project Plan	Within 3 weeks of contract signing	10%
2	Submission and approval of the MDA data Assessment Document, list of priority systems planned to be migrated, , and Data Extraction and Migration Plan.	2 month from contract signing	15%
3	Successful setting up of the testing environment and completion of the initial migration tests.	3 months from contract signing	25%
4	Successful full migration of the agreed 15 applications and submission of Final Migration Report	11 months from contract signing	25%
5	Successful full migration of the next agreed 10 applications and submission of Final Migration Report		20%
5	Delivery of post-migration support and user training	12 months from contract signing	10%

F. CONTRACTING, REPORTING AND VALIDATION PROCEDURE

The Consultant will be contracted by the Public Private Partnership Commission (PPPC) on behalf of the Government of Malawi and the Department of e-Government in particular. All deliverables should be submitted to the focal point from the Department of e-Government, with a copy to Digital Malawi Project Coordinator. Written deliverables should be submitted electronically in PDF and editable Word format, allowing for comments/edits to be made.

The Consultant is expected to work with an assigned Project Specialist on a day-to-day basis, as well as an assignment Project Coordinator at the Department of e-Government that will be the main beneficiary of this assignment.

The Consultant shall be submitting written reports to the Chief Executive Officer, PPPC through the Director for e-Government Department on the activities completed in the agreed work plan. The reports shall be submitted electronically.

G. CLIENT'S RESPONSIBILITIES

The Department of e-Government shall provide the following to the best of their ability:

- All background data and literature considered relevant for accomplishing or informing the assignment and completing identified tasks at their immediate disposal.
- Access to key officials within the relevant Ministries/Agencies/department and other relevant official entities, as applicable.
- Facilitate cooperation from other organizations, whose activities and programs may be considered relevant to the assignment.
- Appropriate office space necessary to carry out the assignment.

H. LOCATION

The National Data Centre is located in Area 4, Lilongwe and will be the primary site. The disaster recovery / secondary / backup site is located in Mandala, Blantyre. A majority of the government ministries, departments and agencies whose data are to be migrated to the National Data Centre are headquartered in Lilongwe.

The Consultant will be expected to be based in Lilongwe, with some limited travel to Blantyre.

I. KNOWLEDGE TRANSFER

Knowledge transfer is considered an integral part of this assignment and should be reflected in the Consultant methodology and technical proposal.

As part of the proposal, the Consultant must provide a training plan that will necessitate knowledge transfer to the local team to enable them manage, maintain, and extend the data migration system after the Consultant's engagement ends. The process needs to be structured and clear to ensure a smooth handover.

The knowledge transfer shall among others include:

1. Define the Scope of Knowledge Transfer
    - Ensure that the local team understands the architecture of the migration system, including databases, ETL (Extract, Transform, Load) tools, scripts, and integrations.
    - Define the data migration processes, including extraction, transformation, validation, and loading.
    - Share detailed information about the tools and technologies used for migration, such as databases, middleware, and any custom scripts or third-party tools.
    - Provide comprehensive documentation covering all aspects of the migration, including system architecture, data mappings, business rules, exception handling, and troubleshooting guidelines.

2. Create Detailed Documentation
    - Prepare technical documentation that should cover system architecture, configurations, environment setups, codebase, and scripts.
    - Document the step-by-step process for data migration, including scheduling, dependencies, and triggers.
    - Prepare data mapping documentation that should include source-to-target mappings, transformation rules, and validation rules.
    - Outline how errors are logged, monitored, and resolved during the migration process.
    - Document test cases, scenarios, and results from pre-migration testing and post-migration validation.
    - List common issues encountered during the migration process and how they were resolved.

3. Hands-on Training Sessions
    - Organize workshops or training sessions where the Consultant walks the team through each aspect of the system. Use both technical and non-technical explanations to cater to different levels of expertise.
    - Let team members shadow the Consultant during live migration activities. Use pair programming for technical tasks like script adjustments or debugging.
    - Set up a sandbox environment where the local team can practice the migration process without impacting live data.

4. Knowledge Transfer Plan
    - Create a phased knowledge transfer plan where the Consultant gradually hands over responsibility, allowing the local team to take on more tasks incrementally.
    - Assign specific team members responsibility for different parts of the system.
    - Have regular checkpoints where the local team demonstrates their understanding by performing certain migration tasks independently under supervision.

5. Documentation Review & Updates
    - Review all documentation with the team. Ensure they understand everything and ask them to provide feedback or identify gaps in their understanding.
    - Encourage the local team to update the documentation during the handover to ensure that it remains relevant and correct.

6. Testing and Validation
    - Ensure the local team can independently set up, run, and troubleshoot the test migration process.
    - Teach the local team how to validate data post-migration, comparing source and target data, and ensuring the integrity and completeness of migrated data.

7. Mentoring and Support
    - Offer continued remote support or mentoring for a period after the official handover. This will allow the team to clarify doubts or troubleshoot any issues that arise after they take full ownership.
    - Set up a shared knowledge repository where documentation, best practices, and common issues can be stored and easily accessed by the team.

8. Final Knowledge Transfer Session
    - Hold a final Q&A session with the local team. Ensure that they can ask any remaining questions or seek clarification on any concepts they are unclear about.
    - Perform a mock migration or simulate a critical part of the process with the local team taking the lead.

9. Evaluation & Feedback
    - Evaluate the local team's understanding by having them explain key concepts or perform a migration task independently.
    - Gather feedback from the local team about the knowledge transfer process. This helps improve future knowledge transfer processes and ensures no critical areas were overlooked.

10. Handover Completion
    - Both the Consultant and the local team should sign off on the knowledge transfer once all topics have been covered, and the team demonstrates readiness to take over the migration tasks.
    - Officially transfer full ownership to the local team once they have successfully completed the migration independently or with minimal support.

J. STAKEHOLDER CONSULTATION

The Consultant is expected to engage in stakeholder consultation to deliver the assignment. The consultations will be key as they will ensure that all relevant parties are involved, their concerns are addressed, and they provide the necessary input and support.

The Consultant will be required to:

- Identify stakeholders with the assistance of the Department of e-Government
- Confirm objectives of stakeholder consultations
- Develop a stakeholder engagement plan
- Prepare for consultations
- Conduct and drive the consultations
- Document consultation outcomes
- Analyze and incorporate feedback
- Manage ongoing stakeholder communication
- Post-migration review
- Close the consultation loop

The Consultant will be required to prepare a and provide a final report to stakeholders summarizing the results of the migration, any issues encountered, how they were resolved, and the final state of the migrated data. This report will be shared with the Department of e-Government.

K. REQUIRED EXPERIENCE: FIRM & CORE TEAM

The bidder shall demonstrate their capacity, expertise, resources, and reliability to execute the assignment. Among others, they must demonstrate the following eligibility standards:

1. Technical Expertise and Skilled Workforce
    - The Consultant should be well-versed in data centre architecture, cloud environments, and hybrid models. They should also have experience working with different hardware, storage, and networking technologies.
    - The Consultant should have a team of certified professionals in key areas such as cloud platforms (AWS, Azure, Google Cloud), data migration tools, automation frameworks, and networking technologies.
    - The Consultant should have a team with experience with different types of databases (relational, NoSQL, etc.), ensuring smooth migration across different systems.
    - The Consultant should have experts in various domains like system architecture, database management, cybersecurity, and data storage.
    - The Consultant should provide copies of CVs including copies of Professional Certifications / Training Certificates for key staff skills required for the assignment.

2. Experience in in data migration
    - Years of experience: The Consultant should have not less than 5 years' relevant experience in data migration projects, especially for data centres.
    - Client References: To demonstrate their experience, the Consultant should be able to provide references from at least three (3) clients where the bidder provided a similar kind of work in the last five (5) years, who can attest to the quality of their services and ability to meet expectations.

3. Testing and Validation Capabilities
    - The Consultant should perform extensive validation and testing to ensure that all data is accurately migrated without corruption or loss.
    - The Consultant should have a strong plan for minimizing downtime and ensuring business continuity during the migration process.

4. Scalability and Support
    - The Consultant should offer scalable migration solutions that can accommodate data growth and changing data requirements.

- The Consultant should be able to customize its approach to meet unique business needs and migration goals rather than providing one-size-fits-all solutions.
- The Consultant should provide post-migration support, including troubleshooting, performance optimization, and ongoing maintenance.

5. Compliance and Security Standards
   - Data Security Certifications: The Consultant should adhere to security standards like ISO/IEC 27001, or SOC 2.
   - Regulatory Compliance: The Consultant should be familiar with industry regulations (e.g., GDPR, CCPA and capable of ensuring the migrated data remains compliant.
   - Electronic Transactions and Cyber Security Act, 2016

6. Project Management Capabilities
   - Structured Approach: The Consultant should offer a clear, structured methodology for managing the migration, including planning, testing, and executing phases.
   - Agile and Flexible: The Consultant should demonstrate their ability to adapt to changes or unforeseen challenges during migration, using project management frameworks like Agile or Waterfall, depending on the needs at hand.
   - Risk Management: The Consultant should have a solid risk assessment and mitigation strategy in place, prepared to handle data integrity, downtime, and security risks.

7. Financial Stability and Reputation
   - Financial Health: The Consultant should demonstrate financial stability, ensuring that it can provide long-term services without interruptions due to financial instability.
   - Reputation in the Market: The Consultant should have a strong reputation in the industry as far as data migration is concerned, with positive feedback from existing clients, and case studies.
   - Incorporation: The Consultant should provide evidence of company registration and tax compliance.

The firm shall propose a core team comprising of at minimum a Project Manager, and 7 technical experts deemed necessary to deliver the assignment. All team members must be fluent in English.

The consulting firm must provide a staffing plan with names, roles, and CVs for the core project team as part of the proposal.

Key Position	Experience	Qualifications
Project Manager (x1)	• Minimum of 5 years' experience in managing IT projects, understanding of project management methodologies, and familiarity with IT systems and technologies • Proven track record of managing end-to-end data centre projects, including data migration	• Minimum of a bachelor's degree in Computer Science / Information Technology / Management Information System or any related field • Must have relevant IT Certifications such as PMP, PRINCE2, Agile/Scrum
Data Analyst (x1)	• Minimum of 3 years' experience in data analysis, data management, or a related role • Proficiency in database management, programming languages, data visualization and statistical analysis	• Minimum of a bachelor's degree in Computer Science / Information Technology / Management Information System / Data Science or any related field • Must have relevant Data Analytics and Visualization Certifications such as Microsoft Certified: Data Analyst Associate, Google Data Analytics Professional Certificate
System Developer (x1)	• Minimum of 3 years' experience in software and systems development, or a related role • Proficiency in programming languages, software development, frameworks & libraries, web development, database management, integrated development environments, and development tools	• Minimum of a bachelor's degree in Computer Science / Information Technology / Software Engineering or any related field • Must have relevant Programming and Software Development Certifications such as Microsoft Certified: Azure Developer Associate, Oracle Certified Professional, Java SE Programmer, AWS Certified Developer – Associate, Python Institute Certification (PCAP or PCPP)

Key Position	Experience	Qualifications
System Tester (x1)	• Minimum of 3 years' experience in software and systems testing, quality assurance or a related role • Proficiency in testing techniques, test management tools & frameworks, scripting languages, database/SQL, and defect tracking tools	• Minimum of a bachelor's degree in Computer Science / Information Technology / Software Engineering or any related field • Must have relevant Software Testing Certifications such as ISTQB Certified Tester, Certified Software Tester (CSTE), Certified Software Test Professional (CSTP)
System Security Specialist (x1)	• Minimum of 3 years' experience in information security, network security or a related role • Proficiency in network security, operating systems security, endpoint security, cryptography, security tools	• Minimum of a bachelor's degree in Computer Science / Information Technology / Cybersecurity or any related field • Must have relevant Certifications such as CISSP, CEH, CISM, GSEC, CompTIA Security+
Hardware Engineer (x1)	• Minimum of 3 years' experience in hardware engineering, hardware installations, hardware support or a related role • Proficiency in hardware designs, computer architecture, hardware configurations, server virtualization, hardware testing, operating systems	• Minimum of a bachelor's degree in Electrical Engineering / Computer Engineering or any related field • Must have relevant IT Certifications such as Certified Network Associate (CCNA), Microsoft Certified: Azure Administrator or equivalent
Network Engineer (x1)	• Minimum of 3 years' experience in network engineering, network installations, network support or a related role	• Minimum of a bachelor's degree in Computer Science / Information Technology / Network Engineering or any related field

Key Position	Experience	Qualifications
	• Proficiency in network concepts, protocols & technologies, network devices, network security, network management tools	• Must have relevant certifications such as CCNA, CCNP, CCIE, CompTIA Network+
Support Officer (x1)	• Minimum of 2 years' experience working in a busy IT environment • Proficiency in operating systems support, computer hardware, software applications, enterprise software	• Minimum of a bachelor's degree in Computer Science / Information Technology or any related field • Must have relevant certifications such as CCNA, CCNP, CDCTP, CompTIA Network+

L. RISK MANAGEMENT

Risk management in this data migration project will be essential to identify, assess, mitigate, and monitor potential risks that could impact the success of the migration project. Proper risk management will ensure that the data migration process is smooth, secure, and meets the project's objectives.

The Consultant must comply with the following risk management measures:

- Risk Identification: Data Loss or Corruption, Downtime and Disruption, Security Breaches, Compatibility Issues, Data Integrity, and Regulatory Compliance
- Risk Assessment: Impact Analysis, Probability Assessment, and Risk Prioritization
- Risk Mitigation: Risk Avoidance, Risk Transfer, Risk Reduction, Risk Acceptance and Contingency Planning
- Risk Monitoring and Control: Regular Monitoring, Early Warning Systems, Mitigation Plan Execution, Regular Reviews, and Communication
- Documentation and Reporting: Risk Register and Risk Reports

M. QUALITY ASSURANCE

Quality assurance in this data migration project will be crucial to ensure that the migrated data is accurate, complete, consistent, and secure. It will involve systematic activities and processes to verify and validate that the data migration meets the project requirements and business objectives.

The Consultant must comply with the following quality assurance measures:

- Data Profiling and Assessment
- Data Cleansing and Transformation

- Data Mapping and Validation
- Testing and Validation: Unit Testing, System Testing, and User Acceptance Testing (UAT) at each stage of migration
- Performance Testing
- Error Handling, Data Reconciliation and Recovery
- Regular Reviews: Regular project reviews and status updates.
- Regulatory Compliance and Data Security
- Audit Trails: Maintain audit trails of the migration process for accountability.
- Documentation and Reporting

N. COMMUNICATION PLAN

A communication plan in this data migration project will be crucial for ensuring that all stakeholders are informed, engaged, and aligned throughout the project. It will help to manage expectations, mitigate risks, and ensure smooth execution.

The Consultant will create a comprehensive communication plan as follows:

- Identify Stakeholders: Project Team, Business Units, Executive Sponsors, End-Users, and External Partners.
- Define Communication Objectives: Awareness, Engagement, Support, and Feedback.
- Determine Communication Methods and Channels: Meetings, Emails, Phone/Video Conferencing, Project Management Tool, Document Repositories, Reports, Documentation, Workshops/Training Sessions, and Surveys/Feedback Forms.
- Establish a Communication Schedule: Kick-off Meeting, Regular Updates, Weekly Meetings, Milestone Meetings, Ad-Hoc Meetings, and Post-Migration Review.
- Define Roles and Responsibilities: Project Manager, Communications Lead, Technical Leads, and Stakeholders.
- Create Communication Content: Project Updates, Technical Updates, Training Materials, and Feedback Summaries.
- Monitor and Evaluate Communication Effectiveness: Feedback Mechanisms, Adjustments, and Success Metrics.
- Documentation: Version Control, maintain detailed documentation of all processes and decisions.

The bidder will maintain Communication Plan, a sample template is captured below:

Communication Type	Audience	Frequency	Purpose	Channel	Owner
Kick-off Meeting					
Weekly Meetings					
Weekly Reports					
Monthly Meetings					
Monthly Reports					
Ad-Hoc Meetings					
Technical Updates					
Stakeholder Updates					
Milestone Meetings					
User Training					
Feedback Surveys					
Post-Migration Review					

ANNEX 1: LIST OF SCOPED GOVERNMENT MINISTRIES, DEPARTMENT AND AGENCIES (MDAs)

Section A: Hosting Requirements

SN	Name of MDA	Existing System(s)
1	Ministry of Health	Malawi Healthcare Information System (MaHIS)
2	Ministry of Health	HIV EMR
3	Ministry of Health	Health Management Information System (HMIS DHIS 2) Platform
4	Ministry of Health	One Health Surveillance Platform (OHSP DHIS 2) Platform
5	Ministry of Health	National Laboratory Information Management System (NLMS)
6	Ministry of Health	Integrated Basic Laboratory Information System (iBLIS)
7	Ministry of Health	Early Infant Diagnostic Platform (EID)
8	Ministry of Health	Online Continuous Professional Development(CPD) Platform
9	Ministry of Health	Integrated Supportive Supervision Platform (ISS)
10	Ministry of Health	Scanform Platform
11	Ministry of Health	Service Level Agreement (SLA -OpenIMIS)
12	Ministry of Health	Port of Entry Surveillance (PoE) System
13	Ministry of Health	Open Logistics Management Information System (OpenLMIS)
14	Ministry of Health	Physical Assets Management Information System (PAM) / Medical Equipment Management Information System (MEMIS)
15	Ministry of Health	eHIN Drug Dispensing System
16	Ministry of Health	Cold Chain Equipment (CCE) Management Information System
17	Ministry of Health	cStock Community Drug Management System
18	Ministry of Health	integrated Community Health Information System (iCHIS)
19	Ministry of Health	mMama Maternal Emergency Support System
20	Ministry of Health	Maternal Death Surveillance System (MatSurv DHIS 2) Platform
21	Ministry of Health	Quality of Care (QoC) MIS
22	Ministry of Health	Tuberculosis EMR
23	Ministry of Health	Malawi Analytics Platform (MAP)
24	Ministry of Health	Finance Management Information System
25	Ministry of Health	integrated Human Resource Management Information System (iHRIS)
26	Ministry of Health	Internal DNS Servers
27	Ministry of Health	Monitoring Tools Interconnector Server

SN	Name of MDA	Existing System(s)
28	Ministry of Health	Staging (Test Server) 1
29	Ministry of Health	Staging (Test Server) 2
30	Ministry of Health	Staging (Test Server) 3
31	Ministry of Health	Staging (Test Server) 4
32	Ministry of Health	Staging (Test Server) 5
33	Ministry of Health	Master Health Facility Registry
34	Ministry of Health	Interoperability Layer
35	Ministry of Health	Master Patient Index Platform
36	Ministry of Health	Terminology Registry
37	Ministry of Health	National Help Desk Platform
38	Ministry of Health	Viral Load Reporting System
39	Ministry of Health	COVID 19 Dashboard (For future emergencies as well)
40	Ministry of Health	Redcap Platform
41	Ministry of Health	Network Controller Server
42	Ministry of Health	RapidPro
43	National Registration Bureau (NRB)	National Registration and Identification System
44	Malawi Bureau of Standards (MBS)	Sanitary and Phytosanitary Information System
45	Ministry of Agriculture	Affordable Inputs Programme (AIP) System

Section B: Colocation Requirements

SN	Name of MDA	Number of Racks / Form Factors	System(s)
1	Malawi Communications Regulatory Authority (MACRA)	6 racks	Domain Controller, Active Directory, Sage, MANS, ASMS, Citrix, CIER Servers, CERT Servers, RAS Servers, Cisco Firewalls and Switches
2	Malawi Revenue Authority (MRA)	1 rack	Disaster Recovery Site for their system National Single Window Project