THE DIGITAL MALAWI ACCELERATION PROJECT

GRANT NUMBER : IDA-E338-MW

PROJECT NUMBER : P505095

TERMS OF REFERENCE

FOR

PROVISION OF MANAGED SERVICES FOR 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 NX-3460-G7 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 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. Both the primary site and the DR site are Tier-III facilities.

The National Data Centre is expected to become fully operational in March 2025. Once the facility becomes operational, it will be expected that there will be smooth, efficient, and secure operation of this critical IT infrastructure. Their importance stems from the growing complexity of data centre operations and the need for specialized expertise.

These terms of reference outline the scope, objectives, methodology and deliverables for the managed services for the National Data Centre of Malawi.

B. BACKGROUND OBJECTIVE

The Department of e-Government intends to use services of a competent and qualified Consulting Firm to provide managed services to its newly commissioned National Data Centre. The managed services for the National Data Centre will provide expert management, cost efficiency, enhanced security, and operational flexibility. These services will help the Government achieve high availability, scalability, and security of applications, systems and data.

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 the managed services for the data centre are:

- To ensure high availability and uptime
- To enhance security and compliance
- To optimize operational efficiency
- To improve scalability and flexibility
- To deliver cost-effective operations
- To provide proactive monitoring and maintenance
- To ensure data backup and disaster recovery
- To simplify it management and reduce complexity
- To improve resource utilization
- To support private cloud integration and hybrid models
- To provide continuous reporting and analytics

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

C. SCOPE OF WORK

The scope of the managed services for the data centre is such that the Consulting Firm ("Consultant") will be responsible for the day-to-day management, maintenance, and optimization of a data centre's IT infrastructure to ensure the efficient, secure, and cost-effective operation of the data centre.

The detailed scope of these works are as follows:

1. Monitoring and Management:
    - 24/7 Monitoring: Continuous surveillance of hardware, network, storage, and security to detect and address issues proactively.
    - Performance Management: Real-time monitoring of the health and performance of IT infrastructure, ensuring optimal functionality and load balancing.
    - Incident Management: Identifying, diagnosing, and resolving issues promptly to prevent downtime and disruptions.

2. Security Management:
    - Firewall and Intrusion Detection/Prevention (IDS/IPS): Implementation and management of security measures to protect the data centre from cyberattacks and unauthorized access.
    - Security Audits and Compliance: Regular assessments of the data centre's security posture, ensuring compliance with industry standards and regulations (e.g., PCI DSS, GDPR, HIPAA).
    - Require compliance with local cybersecurity and data privacy laws and frameworks, such as Malawi's Electronic Transactions and Cyber Security Act.
    - Data Encryption and Backup: Encryption of sensitive data and scheduled backups to ensure data protection and availability.

3. Backup and Disaster Recovery:
    - Data Backup Management: Regularly scheduled backups of critical data and systems to off-site or cloud locations.
    - Disaster Recovery Planning: Development and management of a comprehensive disaster recovery plan, including rapid restoration of services in case of power failure, natural disasters, or cyberattacks.
    - Failover Solutions: Ensuring high availability by providing backup systems and networks that can take over in the event of an outage.
    - Recovery Point Objective (RPO): 15 minutes to a 1 hour.
    - Recovery Time Objective (RTO): 1 hour to 3 hours.

4. Infrastructure Management:
    - Hardware Management: Procurement, installation, maintenance, and lifecycle management of servers, storage, and network equipment.
    - Capacity Planning: Ensuring that the data centre has adequate resources to handle current workloads and future growth, including the allocation of storage, processing power, and network bandwidth.
    - Patching and Updates: Regular updates and patches for servers, applications, and networking equipment to maintain security and functionality.

5. Network Management:
    - Network Performance Optimization: Ensuring low-latency, high-bandwidth connections between servers, storage, and users.
    - Load Balancing: Distributing network traffic across multiple servers to prevent overload and ensure efficient utilization of resources.
    - Virtual Private Network (VPN) Management: Establishing and managing secure VPN connections for remote users and branch offices.

6. Power and Cooling Management:
    - Power Management: Managing power supply, backup generators, and Uninterruptible Power Supply (UPS) systems to ensure constant operation and minimize downtime.

- Cooling Systems Optimization: Monitoring and managing HVAC systems to maintain optimal environmental conditions (temperature and humidity) for data centre equipment.
- Energy Efficiency Initiatives: Implementing green energy solutions and optimizing power usage to reduce operational costs.

7. Storage Management:
   - Storage Provisioning: Managing and optimizing storage resources, including NAS (Network Attached Storage), SAN (Storage Area Networks), and cloud storage solutions.
   - Data Tiering: Automating the movement of data between high-performance and low-cost storage tiers to ensure efficiency.
   - Data Retention Policies: Ensuring compliance with data retention regulations and implementing policies to handle archival and deletion of obsolete data.

8. Cloud Integration and Hybrid Solutions:
   - Cloud Management Services: Managing cloud infrastructure (public, private, or hybrid) to ensure seamless integration with on-premise data centre resources.
   - Hybrid Cloud Solutions: Designing and managing hybrid environments that leverage both on-premises data centre resources and cloud services.
   - Migration Services: Assisting in the migration of data, applications, and workloads to cloud platforms or between data centres.

9. Compliance and Reporting:
   - Compliance Management: Ensuring the data centre meets regulatory requirements (e.g., ISO 27001, SOC 2, PCI DSS) through regular audits and risk assessments.
   - Reporting and Analytics: Providing real-time and periodic reports on data centre performance, security incidents, and capacity usage to keep stakeholders informed.
   - Electronic Transactions and Cyber Security Act, 2016

10. Support and Help Desk:
    - Technical Support: Providing on-demand support for troubleshooting hardware, software, and network issues.
    - Help Desk Services: Offering 24/7 help desk services for end-users or IT teams, resolving user issues or service requests efficiently.
    - On-Site and Remote Support: Offering both on-site technical teams for hands-on support and remote assistance for routine tasks.

11. Vendor and Asset Management:
    - Vendor Coordination: Managing relationships with hardware and software vendors, including negotiating contracts, handling warranties, and coordinating repairs.
    - Asset Tracking: Keeping a record of data centre assets, including hardware, software licenses, and network components, to ensure efficient utilization and cost management.

12. Automation and Orchestration:
    - Automated Provisioning: Implementing automated workflows for resource provisioning (e.g., compute, storage, network) to speed up service delivery.
    - Orchestration Tools: Utilizing orchestration tools to manage complex workflows, automate routine tasks, and streamline operations across multi-cloud or hybrid environments.

13. Scalability and Future Planning:
    - Scalability Management: Ensuring the infrastructure can scale easily in response to growing business needs, either through cloud resources or additional hardware.
    - Technology Roadmap: Assisting in the development of long-term technology strategies to ensure the data centre remains up-to-date with the latest technologies and industry trends.

14. Subsequent Migration of data for MDAs:
    - Detailed assessments, data classification, and development of a comprehensive migration roadmap during year 2 of operation, following the initial data migration activities.
    - 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.

15. Adherence of the guiding Framework for Service Delivery:
    The Consulting Firm will be required to deliver this service under the ITIL for IT Service Management through:
    - Service Strategy, whose key activities are:
        - Service Portfolio Management
        - Demand Management
    - Service Design, whose key activities are:
        - Service Catalog Management
        - Service Level Management
        - Risk Management
        - Availability Management
        - Capacity Management
        - Information Security Management
        - Vendor / Supplier Management
    - Service Transition, whose key activities are:

    - Change Management
    - Release and Deployment Management
    - Asset and Configuration management
    - Knowledge Management
- Service Operation, whose key activities are:
    - Event Management
    - Incident Management
    - Problem Management
    - Access Management
    - Facilities Management
    - Request Fulfilment
- Continual Service Improvement, whose key activities are:
    - Process Evaluation
    - Improvement Initiatives

16. RACI Matrix:
    For each of the ITIL processes, the Consulting Firm will be required to develop a RACI Matrix to define roles and responsibilities, ensuring that everyone involved knows their specific roles. The roles in the matrix will be categorized as follows:
    - **R (Responsible):** The person or team who perform the task.
    - **A (Accountable)**: The person who owns the work; is ultimately accountable for the task's completion; and has decision-making authority.
    - **C (Consulted)**: People who provide input and feedback on the task. They are usually subject-matter experts whose opinions are required for successful task completion.
    - **I (Informed)**: People who are kept updated on progress and outcomes but are not directly involved in the work.

D. EXPECTED DELIVERABLES

The Consultant is expected to submit the following deliverables:

No	Nature of Report	Description of Sub Reports	Submission Frequency
1	Inception Report	Inception Report including work plan, timelines, SLAs for the service desk and Standard Operating Procedures (SOP)s for Service Desk. This report is to be approved by the Client.	Once off; at Inception
2	Infrastructure Installation Completion Report	Report to include scope of work, hardware details, software details, network configurations, monitoring tools, facilities, environmental report, and sign-off. This report is to be approved by the Client.	Once off; once installation of infrastructure is completed
3	ITIL Structure Report	Report to detail the ITIL best practices to effectively manage, monitor, and deliver IT services to the client.	Once off; at Inception

No	Nature of Report	Description of Sub Reports	Submission Frequency
		The report to include the RACI Matrix. This report is to be approved by the Client.	
4	Performance Reports	Uptime and Availability Report: Details the uptime percentage of the data centre and highlights any instances of downtime or outages to measure SLA compliance.	Daily, Weekly, Monthly
		Resource Utilization Report: Provides insights into the usage of CPU, memory, storage, and network bandwidth to help optimize resource allocation and identify underutilized or overburdened resources.	Daily, Weekly, Monthly
		Capacity Planning Report: Forecasts future resource requirements based on current usage trends, helping to ensure that the data centre can scale appropriately to meet growing demands.	Monthly
5	Incident Reports	Incident Summary Report: Details all incidents that occurred during a specific period, including hardware failures, software issues, and network problems. The report should include the root cause, impact analysis, and resolution times.	Adhoc; as and when an incident occurs Monthly
		Root Cause Analysis (RCA) Report: Provides a detailed analysis of major incidents, outlining the cause of the issue and the steps taken to resolve it. It also highlights measures to prevent similar incidents in the future.	Adhoc; as and when an incident occurs Monthly
		Incident Response and Resolution Times: Tracks the time taken to respond to and resolve incidents, ensuring adherence to SLAs and helping improve future response times.	Adhoc; as and when an incident occurs Monthly
6	Security Reports	Vulnerability Assessment Report: Lists any vulnerabilities identified during security scans, detailing their severity and the actions taken to mitigate them.	Weekly, Monthly
		Intrusion Detection and Prevention Report: Summarizes any security incidents, including attempted breaches, malware detection, and unauthorized access attempts. The report outlines how these threats were detected and resolved.	Daily, Weekly, Monthly
		Firewall and Network Security Report: Provides a comprehensive overview of firewall activity, including blocked traffic, intrusion attempts, and security rule changes.	Daily, Weekly, Monthly

No	Nature of Report	Description of Sub Reports	Submission Frequency
		Patch Management Report: Lists all patches applied to systems and software during the reporting period, ensuring that vulnerabilities are being addressed in a timely manner.	Adhoc; as and when a patch is applied Monthly
		User Access Report: Details who has accessed the data centre systems and when, providing audit trails for user activity and compliance purposes.	Daily, Weekly, Monthly
7	Backup and Disaster Recovery Reports	Backup Status Report: Outlines the status of all scheduled backups, including any failures, incomplete backups, and successful ones. This report ensures that critical data is being protected regularly.	Daily, Weekly, Monthly
		Recovery Point Objective (RPO) and Recovery Time Objective (RTO) Reports: Evaluates the ability to recover data within the agreed-upon time frames and objectives.	Adhoc; as and when data is recovered Monthly
		Disaster Recovery Test Report: Details the results of any disaster recovery tests, identifying any gaps in recovery processes and recommendations for improvement.	Adhoc; as and when DR test is done Monthly
8	Compliance and Audit Reports	Regulatory Compliance Report: Ensures the data centre complies with industry standards such as ISO 27001, GDPR, PCI DSS, HIPAA, and other applicable regulations. This report includes audit logs, security controls, and adherence to data protection standards.	Monthly
		Audit Trail Report: Tracks changes to critical systems, files, and configurations, providing an audit trail for compliance and forensic purposes in the event of a security breach.	Weekly, Monthly
		Data Retention Report: Summarizes how long data is stored, what data has been archived or deleted, and compliance with data retention policies.	Monthly
9	Energy and Environmental Reports	Energy Consumption Report: Details the energy usage of the data centre, including power usage effectiveness (PUE) and other efficiency metrics, helping to optimize energy consumption and reduce costs.	Daily, Weekly, Monthly
		Cooling and HVAC Performance Report: Monitors the performance and efficiency of the heating, ventilation, and air conditioning (HVAC) systems, ensuring the data centre operates within the optimal temperature and humidity levels.	Daily, Weekly, Monthly
		Carbon Footprint Report: Calculates the environmental impact of data centre operations,	Weekly, Monthly

No	Nature of Report	Description of Sub Reports	Submission Frequency
		including emissions related to energy consumption, and suggests measures to reduce carbon footprint.	
10	Operational and Maintenance Reports	Hardware Health and Lifecycle Report: Monitors the status of all physical hardware, highlighting potential failures, needed upgrades, and scheduled maintenance. This report ensures equipment is performing optimally and can help plan for hardware replacement.	Daily, Weekly, Monthly
		Maintenance Activity Report: Tracks all scheduled and unscheduled maintenance activities, detailing the scope of work, affected systems, and outcomes. This report helps in ensuring continuous operation and minimizing downtime.	Adhoc; as and when a maintenance activity is done Monthly
		Change Management Report: Provides a record of all changes made to the data centre's infrastructure, including system upgrades, configuration changes, and software updates. This report helps in managing risks associated with changes and ensures proper testing and approval processes.	Adhoc; as and when a change is effected Monthly
11	SLA Compliance Reports	Service Level Agreement (SLA) Report: Measures performance against agreed service levels, such as uptime, response times, and resolution times. This report helps ensure that the managed service provider is delivering services in line with contractual obligations.	Weekly, Monthly
		Downtime Report: Provides a breakdown of any downtime experienced, the cause, and how it was resolved, showing compliance with uptime guarantees specified in the SLA.	Adhoc; as and when a downtime is experienced Monthly
12	Cloud and Hybrid Management Reports	Cloud Resource Utilization Report: Tracks the usage of cloud resources in hybrid or multi-cloud environments, providing insights into cost optimization and performance.	Daily, Weekly, Monthly
		Cloud Integration Performance Report: Details the performance and efficiency of cloud integrations, including data transfers, latency, and uptime for cloud-based applications.	Weekly, Monthly
		Cloud Spend Report: Provides a detailed breakdown of cloud costs, helping organizations understand their spending and identify areas for optimization.	Monthly
13	Automation and	Automation Performance Report: Tracks the effectiveness of automation tools used within the data	Monthly

No	Nature of Report	Description of Sub Reports	Submission Frequency
	Orchestration Reports	centre, highlighting tasks that were automated, the time saved, and any issues encountered.	
		Orchestration Report: Monitors the performance of orchestration tools that manage multi-cloud or hybrid environments, providing insights into workload distribution and optimization.	Monthly
14	Vendor and Asset Management Reports	Vendor Performance Report: Evaluates the performance of third-party vendors, including hardware, software, and service providers, ensuring that they meet their contractual obligations.	Monthly
		Asset Inventory Report: Provides a detailed inventory of all physical and virtual assets in the data centre, helping to track the status, location, and lifecycle of each asset.	Monthly
		Warranty and Support Contract Report: Tracks the status of hardware warranties and support contracts, ensuring that they are up-to-date and cover all critical systems.	Monthly

The format for report deliverables should take any of the following formats depending on content and usage:

	Description	Format	Content
1	Document-Based Reports	• PDF (Portable Document Format) • DOCX (Microsoft Word) • HTML (Web-Based Reports)	• Formal and detailed reports • Reports with textual explanations with tables and graphs • Interactive reports for online access
2	Spreadsheet-Based Reports	• XLSX (Microsoft Excel) • CSV (Comma-Separated Values)	• Detailed numerical data (e.g., uptime, resource utilization) • Trend analysis over specific periods • Pivot tables for dynamic data filtering • Forecasting models based on historical performance
3	Dashboard & Visualization Reports	• PowerPoint (PPTX) • BI Tools (Power BI, Tableau, Grafana, etc.) • Infographics (PNG, SVG, JPEG)	• Summary-level reports for presentations • Interactive dashboards • Quick and visual summaries
4	Email-Based Reports	• HTML emails with embedded charts and	• Weekly snapshots of data centre health

	Description	Format	Content
		summaries • PDF or Excel attachments	• Incident summaries and resolutions • Automated alerts for SLA violations
5	Real-Time Monitoring Reports	• Web-based portals with live data feeds • API-based reports (JSON, XML)	• Live metrics (power consumption, cooling efficiency, server utilization) • Threshold alerts and notifications • Customizable views for different stakeholders

E. SCHEDULE OF COMPLETION

The Consultant is expected to complete the assignment in full within thirty-six (36) calendar months based on the indicative timelines and payment schedule detailed below:

S/No	Milestone/deliverable	Timeline	Payment Schedule
1	a) Submission of Inception report b) Acceptance of Installation and Configuration of setup (e.g., provisioning of hardware, network setup, monitoring tools, etc.) c) Infrastructure Installation Completion Report	Within 4 weeks of contract signing	The agreed once-off Initial Setup Fees
2	Submission of all reports due based on the Schedule of Expected Deliverables	25th day of each month	The agreed monthly recurring charge

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. All deliverables should be submitted to National Data Centre 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 National Data Centre 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 Director for e-Government Department for certification for payment before submission to the Chief Executive Officer, PPPC 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 hosted in 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. CONTRACTING DURATION

The contract will run for thirty-six (36) calendar months with a total level of input of 3663-man days for key experts renewable upon satisfactory performance.

J. KNOWLEDGE TRANSFER

Knowledge transfer from the Consulting Firm to the technical team of the government is crucial to ensure that internal teams understand the infrastructure, processes, and configurations in place. This helps maintain continuity and reduces the risk of service disruption when the consultant transitions out of their role.

Knowledge transfer initiatives should be reflected in the Consultant methodology and technical proposal. The process needs to be structured and clear to ensure a smooth handover.

The knowledge transfer shall among others include:

1. Infrastructure Documentation
    - Detailed maps of data centre networks, including topology, IP addressing, VLANs, and connection points.
    - List of all equipment, including servers, switches, firewalls, storage units, power supplies, etc., along with their serial numbers, locations, and warranties.
    - Physical placement of hardware within the racks.
    - Fibre and copper cabling maps, showing patch panels, ports, and pathways.

2. Configuration Documentation
    - Operating systems, patches, virtual machines, hypervisors, and their settings.
    - Router, switch, and firewall configurations, including routing tables, access control lists (ACLs), and security settings.
    - SAN/NAS setups, RAID configurations, and storage allocations.

- Backup schedules, tools used, restore points, and disaster recovery procedures.

3. Operational Procedures
   - Step-by-step guides for regular tasks, such as adding users, updating systems, monitoring services, or troubleshooting common issues.
   - Detailed instructions on how to handle critical incidents (e.g., hardware failures, network outages, security breaches).
   - Key performance metrics, uptime requirements, response times, and resolution procedures.

4. Security Policies
   - Permissions for accessing different parts of the data centre, servers, and network devices.
   - Overview of password policies and access credentials for critical systems.
   - Documentation on security monitoring systems and procedures for analyzing logs.

5. Technical Training for IT Teams
   - 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
   - Hands-on training on managing and configuring servers, network devices, and storage systems.
   - Training on using monitoring tools (e.g., Nagios, SolarWinds, etc.), checking system health, analyzing logs, and troubleshooting performance issues.
   - Sessions focused on running and testing backup and disaster recovery plans, ensuring the internal team knows how to restore systems from backups and handle failover.
   - Walk-throughs on data centre security protocols, including patch management, vulnerability scanning, and incident response.
   - Training on how to handle first-level issues, escalation protocols, and monitoring alerts.
   - Training on service request procedures, expectations on downtime, and communication channels during incidents.

7. Access Transfer
   - Transfer of all administrative credentials (e.g., root access, network device logins) with clear instructions on changing passwords post-handover.
   - Modifying or revoking the consultant’s access to the data centre and systems post-transition.
   - Ensure internal teams or the new provider have access to management consoles, cloud platforms, and monitoring dashboards.

8. Key Processes & Automation
   - Handover of any scripts or automation tools created for the data centre, such as deployment automation, network management, or monitoring configurations.

- Explanation of how to modify or update any automated workflows, such as provisioning virtual machines or patch management systems.

9. Knowledge Base & Historical Context
   - Consolidation of all relevant articles, manuals, SOPs, and guides into a central repository, or knowledge management system accessible by the team.
   - Review of past changes made to the data centre infrastructure (e.g., upgrades, migrations), including explanations of why they were made.
   - Documentation of major incidents, root causes, and lessons learned to help the new team anticipate and avoid similar issues.

10. Operational Handoff
    - For 24/7 data centre operations, ensure that shift handover processes are clear and well-documented to maintain continuous operations.
    - Documentation of relationships with hardware and software vendors, including support contracts, points of contact, and maintenance agreements.
    - Set up dashboards and alerts to ensure that performance, capacity, and security are being monitored. Train the team on how to interpret and act on monitoring data.

11. Final Review and Knowledge Gaps
    - Conduct a final review meeting with the managed service consultant and the internal team or new service provider to ensure all critical knowledge has been transferred.
    - Identify any remaining knowledge gaps and ensure they are closed with additional training or documentation.
    - Have both parties sign off on the knowledge transfer process to ensure all necessary information has been transferred and is understood.

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
   - Certified Staff: The firm should have professionals with certifications in relevant technologies and platforms, such as: Cisco Certified Network, Professional (CCNP), VMware Certified Professional (VCP), Microsoft Certified Solutions Expert (MCSE), Certified Information Systems Security Professional, (CISSP), AWS Certified Solutions Architect (for cloud integration), and CompTIA Data Centre Certification
   - The firm should provide copies of CVs including copies of Professional Certifications / Training Certificates for key staff skills required for the assignment.
   - Vendor Certifications: The firm should be certified as partners or specialists by major technology vendors (e.g., Cisco, HP, Dell, Microsoft, IBM, Oracle, AWS, Google Cloud, and others). These partnerships ensure they have the knowledge and tools to manage the specific hardware or software used in your data centre.

2. Experience in Data Centre Operations
    - Years of experience: The firm should have not less than 5 years' relevant experience of managing data centres.
    - Client References: To demonstrate their experience, the firm should be able to provide references from at least three (3) clients where the bidder provided a similar kind of work in the last three (3) years, who can attest to the quality of their services and ability to meet expectations.
    - Case Studies: the firm must demonstrate past success in managing similar data centre operations, handling complex challenges, or delivering unique solutions in specific industries.

3. Security Expertise
    - Cybersecurity Skills: The firm should have a strong focus on data centre security, with specialists in areas such as: Network Security (e.g., firewalls, IDS/IPS systems), Data Encryption, Identity and Access Management (IAM), and Disaster Recovery and Business Continuity Planning (BCP)
    - Security Operations Centre (SOC): If applicable, the firm should have a dedicated SOC that monitors security threats 24/7 and responds to incidents in real-time.

4. 24/7 Monitoring and Support Capabilities
    - The firm should offer 24/7/365 monitoring and support to ensure data centre availability and rapid incident response. This should include: Help Desk Support (with defined Service Level Agreements or SLAs), Network and Infrastructure Monitoring and Incident Response and Resolution

5. Service Level Agreements (SLAs)
    - The firm should offer tailored SLAs to meet your organization's uptime, performance, and incident response needs. SLAs should include:
        - Uptime Guarantees: (e.g., 99.9% or higher availability)
        - Incident Response Times: Clearly defined response and resolution times based on the severity of incidents.
        - Penalties for Non-Compliance: Ensuring that the firm is accountable for meeting the agreed-upon performance standards.

6. Scalability and Flexibility
    - Scalable Services: The firm should be capable of scaling its services up or down based on your data centre's changing needs. This includes adding additional storage, compute power, or bandwidth as needed.
    - Hybrid and Cloud Integration Expertise: The ability to manage hybrid infrastructures (combining on-premises and cloud resources) or integrate with public clouds (e.g., AWS, Azure, Google Cloud) is an important qualification for modern data centre operations.

7. Disaster Recovery and Business Continuity Planning
    - Disaster Recovery Expertise: The firm should have experience designing, implementing, and testing disaster recovery (DR) plans to ensure data and applications can be quickly restored in case of an outage or disaster.
    - Data Backup Capabilities: The firm should provide robust backup services with automated scheduling, secure storage (on-site, off-site, or cloud-based), and rapid data restoration.

8. Automation and Orchestration Capabilities
    - Automation Tools and Frameworks: The firm should employ tools and best practices for automating routine data centre tasks (e.g., server provisioning, backup management, patching) to improve efficiency and reduce human error.
    - Orchestration Platforms: If your data centre involves hybrid or multi-cloud environments, the firm should have the ability to manage and orchestrate workloads across these environments to optimize performance and cost.

9. Compliance and Regulatory Knowledge
    - Compliance Certifications: The firm should have a deep understanding of relevant compliance standards and regulations, such as: ISO 27001 (Information Security Management), SOC 2 (System and Organization Controls), PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act), and GDPR (General Data Protection Regulation) if applicable in regions like the EU.
    - Audit and Reporting Capabilities: The firm should have experience conducting regular audits and maintaining compliance with data privacy laws and security regulations.

10. Advanced Reporting and Analytics
    - Performance and Utilization Reports: The firm should provide detailed reports on system performance, resource utilization, and capacity planning to help optimize data centre operations.
    - Security and Compliance Reporting: Regular reporting on security status, vulnerabilities, and compliance with regulatory standards should be provided.
    - Cost Management and Forecasting: The firm should provide financial reports that track costs and help forecast future needs, particularly for cloud resources or hybrid environments.

11. Vendor and Asset Management
    - Vendor Management Expertise: The firm should have experience managing relationships with third-party vendors (e.g., hardware and software suppliers), ensuring smooth operations and timely support.

12. Proven Transition and Onboarding Process
    - Clear Onboarding Plan: The firm should have a structured onboarding process to smoothly transition your data centre to their managed services, ensuring minimal disruption to ongoing operations.
    - Change Management Expertise: They should have a solid change management framework to manage transitions, upgrades, or changes without affecting business continuity.

13. Financial Stability and Reputation
    - Financial Health: The firm should demonstrate financial stability, ensuring that it can provide long-term services without interruptions due to financial instability.
    - Reputation in the Market: The firm should have a strong reputation in the industry for delivering managed services, with positive feedback from existing clients, case studies, and industry awards or certifications.
    - Incorporation: The firm should provide evidence of company registration and tax compliance.

14. Standards and Tools
    - The firm should indicate the standards, tools, and configurations that they will deploy during the execution of this assignment. Refer to Annex 1.

The firm shall propose a core team comprising of at minimum a Service Delivery Manager, and 12 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
Service Delivery Manager (x1)	• Minimum of 5 years' experience in service delivery management, preferably within a data centre, cloud infrastructure, or managed services environment. • Proven track record of managing SLAs, operational teams, and client relationships in a managed services setting.	• Minimum of a bachelor's degree in Information Technology, Computer Science, Business Administration, or a related field. • Must have relevant IT Certifications such as ITIL, Project Management certification (e.g. PMP, PRINCE2).

Key Position	Experience	Qualifications
IT Operations Analyst (x1)	• Minimum of 5 years' experience in IT change management, preferably in a data centre or managed services environment. • Proficiency in data centre infrastructure, including servers, networking, storage, and virtualization technologies.	• Minimum of a bachelor's degree in in Information Technology, Computer Science, or a related field. • Must have relevant IT Certifications such as CompTIA Server+ or Network+, VMware Certified Professional (VCP), Cisco Certified Network Associate (CCNA), Microsoft Certified: Azure Administrator or equivalent.
Change Analyst (x1)	• Minimum of 3 years' experience in IT operations, system administration, or data centre management. • Proven track record in managing large-scale changes in complex technical environments, including infrastructure, networking, and cloud technologies.	• Minimum of a bachelor's degree in Information Technology, Computer Science, or a related field. • Must have relevant IT Certifications such as ITIL, Project Management certification (e.g. PMP, PRINCE2).
Applications Administrator (x1)	• Minimum of 3 years' experience as an Applications Administrator, Systems Administrator, or in a similar role in a data centre or IT environment. • Familiarity with operating systems (Linux, Windows) and database systems (SQL, Oracle), networking concepts, virtualization, and cloud computing.	• Minimum of a bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as ITIL, CompTIA Server+, Microsoft Certified: Azure Administrator, Red Hat Certified System Administrator (RHCSA), or similar certifications.

Key Position	Experience	Qualifications
Database Administrator (x1)	• Minimum of 3 years' experience as a Database Administrator in an enterprise or data centre environment. • Proficiency in SQL and database performance tuning techniques, database administration tools, monitoring platforms, backup and recovery strategies, disaster recovery planning, high availability configurations, automation and scripting tools.	• Minimum of a bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as ITIL, Oracle Certified Professional (OCP), Microsoft Certified: Azure Database Administrator, or other relevant certifications.
Systems Administrator (x1)	• Minimum of 3 years' experience as a Systems Administrator in a data centre or enterprise environment. • Proficiency with server hardware, storage systems, network configurations, automation and scripting tools, monitoring tools, cloud environments, hybrid cloud architecture, storage systems, and virtualization platforms.	• Minimum of a bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as Microsoft Certified: Windows Server, Azure Administrator, Red Hat Certified System Administrator (RHCSA), Linux Professional Institute Certification (LPIC), VMware Certified Professional (VCP) or equivalent certification.
Storage Administrator (x1)	• Minimum of 3 years' experience as a Storage Administrator or in a similar role managing enterprise storage systems in a data centre environment. • Strong understanding of storage protocols, storage virtualization technologies, storage management tools,	• Minimum of a bachelor's degree in Information Technology, Computer Science, or a related field, or equivalent experience. • Must have relevant IT Certifications such as EMC Proven Professional or NetApp Certified Data Administrator, CompTIA

Key Position	Experience	Qualifications
	backup and recovery tools, scripting languages.	Storage+ or similar storage certifications, VMware Certified Professional or other relevant virtualization certifications.
Capacity Planner (x1)	• Minimum of 3 years' experience in capacity planning, infrastructure management, systems administration, or a related field in a data centre or IT environment. • Familiarity with monitoring tools and capacity planning software (e.g., SolarWinds, Nagios, VMware vCentre, etc.), data centre infrastructure components, including servers, storage, networking, and power systems.	• Minimum of a bachelor's degree in Computer Science, Information Technology, Engineering, or a related field, or equivalent experience. • Must have relevant IT Certifications such as ITIL, CompTIA Data Centre+, Certified Data Centre Management Professional (CDCMP), or similar relevant certifications.
Data Centre Technician (x1)	• Minimum of 2 years of hands-on experience working in a data centre environment or in IT hardware support roles. • Proficient in hardware troubleshooting and repair, including knowledge of server architecture, storage systems, networking hardware and operating systems.	• Minimum of a diploma in Information Technology, Computer Science, or a related field is preferred, but relevant experience can substitute. • Must have relevant IT Certifications such as CompTIA Server+, A+, Network+, or other relevant IT certifications.
Quality Assurance Tester (x1)	• Minimum of 3 years' experience as a Quality Assurance Tester, preferably in a data centre or enterprise IT environment. • Proficient in automated testing tools, scripting	• Minimum of a bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as ISTQB

Key Position	Experience	Qualifications
	languages, performance testing and monitoring tools, data centre infrastructure, CI/CD pipelines and integration of automated testing frameworks into development workflows.	Certified Tester, automated testing tools, ITIL Foundation or similar certifications.
Network Architect (x1)	• Minimum of 3 years' experience in network architecture, design, and engineering, preferably in a data centre or enterprise IT environment. • Proficient in networking protocols, Layer 2/Layer 3 switching, routing, network devices, network security best practices, firewall configurations, VPNs, access controls, encryption technologies, network management, monitoring tools, network virtualization, SDN technologies, cloud networking, VPC design and hybrid connectivity solutions.	• Minimum of a bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as Cisco Certified Internetwork Expert (CCIE) or Cisco Certified Network Professional (CCNP), Juniper Networks Certified Internet Specialist (JNCIS), VMware Certified Professional – Network Virtualization (VCP-NV), Certified Information Systems Security Professional (CISSP) for network security expertise, or similar certifications.
Systems Security Officer (x1)	• Minimum of 3 years' experience in IT security, with a focus on infrastructure, systems, or data centre security. • Strong knowledge of security frameworks, network security principles, firewalls, VPNs, encryption, intrusion detection/prevention systems, security tools, multi-factor authentication, security monitoring, log	• Minimum of a bachelor's degree in Information Security, Computer Science, Information Technology, or a related field, or equivalent experience. • Must have relevant IT Certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Ethical Hacker

Key Position	Experience	Qualifications
	analysis, and incident response.	(CEH), CompTIA Security+ or other security-related certifications.
Telecoms Engineer (x1)	• Minimum of 3 years' experience in telecommunications engineering, with a focus on data centres or large-scale IT infrastructures. • Strong knowledge of telecommunications systems, PBX, VoIP, SIP, SS7, telecom protocols, networking technologies, wireless communication technologies, satellite communication systems, telecom management, monitoring tools, fibre optics, RF systems, and cellular networks.	• Minimum of a bachelor's degree in Telecommunications, Electrical Engineering, Computer Science, or a related field, or equivalent experience. • Must have relevant IT Certifications such as Certified Telecommunications Network Specialist (CTNS), Cisco Certified Network Associate (CCNA) – Voice or Collaboration, CompTIA Network+, Certified Wireless Network Professional (CWNP), or similar networking certifications.

•

L. COMMUNICATION PLAN

A communication plan for managing services of a data centre will ensure that all stakeholders remain informed, engaged, and aligned throughout the lifecycle of the service. A clear plan will outline how information will be shared, the communication channels, frequency, and the responsibilities of both the managed services provider and the Client.

The bidder will create a comprehensive communication plan that will be structured as follows:

a) Objectives

The Consulting Firm will stipulate the purpose of this communication plan that is to:

- Facilitate clear, timely, and effective communication between all parties involved in the data centre managed services.
- Ensure transparency on service performance, incidents, and operational updates.
- Establish regular reporting mechanisms to monitor service levels and key performance indicators (KPIs).
- Provide a process for addressing and escalating issues.

b) Key Stakeholders
   - Identify the key stakeholders for communication. This includes both internal and external parties:
     - Client Stakeholders: IT Operations Team, Data Centre Administrators, Business Unit Heads, and Executives
     - Service Provider Stakeholders: Account Manager, Technical Support Team Network and Infrastructure Engineers, Service Desk, and Senior Management

c) Communication Methods & Channels
   The Consulting Firm will determine the different communication methods that will be used based on the type of information being conveyed, the urgency, and the audience. These include:
   - Email: For regular updates, service reports, and general notifications.
   - Virtual: For urgent issues, escalations, or high-priority meetings.
   - Incident Management Platform: To track service tickets, changes, and incidents in real-time.
   - Service Portal: For self-service access to monitoring, reporting, and change management.
   - In-person Meetings: For quarterly reviews, major changes, or strategic planning.

d) Communication Schedule
   The Consulting Firm will adopt a communication schedule to be used during the assignment. A sample template is captured below:

Type of Communication	Purpose	Audience	Frequency	Channel / Method	Owner
Service Kick-off Meeting	Introduce stakeholders, review scope, discuss SLAs and expectations	Client and Service Provider Stakeholders	Once-off; at project start	In-person / Virtual	Project Manager
Weekly Status Reports	Provide updates on service performance, issues, ongoing tasks	IT Operations Team, Account Manager	Weekly	Email	Service Delivery Manager
Monthly Service Review	Review SLA performance, incident metrics, and improvements	IT Operations Team, Business Unit Heads	Monthly	Email / Virtual	Account Manager
Incident Notifications	Notify about critical incidents or service disruptions	IT Operations, Service Desk, Senior Management (based on severity)	As required (within SLA)	Incident Management Platform / Phone / Virtual	Service Desk Lead

Type of Communication	Purpose	Audience	Frequency	Channel / Method	Owner
Change Management Meetings	Review and approve planned changes in the data centre	IT Operations Team, Engineers	Weekly or as needed	In-person / Virtual	Change Manager
Quarterly Business Review (QBR)	Strategic review of service performance, improvements, upcoming needs	Executives, Senior Management	Quarterly	In-person / Virtual	Account Manager
Ad-hoc Communication	Urgent issues, escalations, or unscheduled matters	Relevant stakeholders (IT Ops, Senior Management)	As required	In-person / Virtual / Email	Varies

e) Communication Content
The Consulting Firm will ensure that the various communications will bear relevant content based on the purpose of the communication. For instance:

- Service Reports (Weekly/Monthly):
  - Summary of key activities
  - SLA performance (uptime, response times, resolution times)
  - Incident reports
  - Planned maintenance or changes
  - Upcoming service improvements

- Incident Notifications:
  - Description of the issue
  - Impacted services and estimated downtime
  - Steps being taken to resolve the issue
  - Expected resolution time
  - Final incident resolution report (after the issue is resolved)

- Change Management:
  - Description of the change (e.g., hardware upgrade, software patch)
  - Impact analysis (potential downtime or disruption)
  - Rollback plan
  - Approval status

- Quarterly Business Review (QBR):
  - Review of past performance against agreed SLAs and KPIs
  - Major incidents and root cause analysis
  - Improvements made and future plans
  - Client feedback and business objectives alignment
  - Future capacity planning and upgrades

f) Escalation Process

The Consulting Firm will devise an escalation process that will be followed in the event of issues or failures that require escalation.

- Level 1 Escalation (Service Desk):
  - Initial issue reporting and troubleshooting.
  - Response time: As defined in the SLA

- Level 2 Escalation (Technical Support/Engineers):
  - In case the issue is unresolved at Level 1, it will be escalated to engineers for more in-depth analysis.
  - Response time: As defined in the SLA

- Level 3 Escalation (Senior Management):
  - If the issue is critical or not resolved at Level 2, escalate to senior management for decision-making or approval of further action.
  - Response time: As defined in the SLA

g) Roles and Responsibilities

Roles	Responsibilities
Service Delivery Manager	Oversee service delivery and ensure SLA compliance. Coordinate with stakeholders.
Account Manager	Act as the main point of contact for the client, handle relationship management and escalations.
IT Operations Team	Monitor day-to-day operations, handle incidents, and coordinate with the service provider.
Change Manager	Coordinate all changes and ensure proper documentation and approval.
Service Desk	First point of contact for incidents, manage ticketing, and initial troubleshooting.
Senior Management	Provide strategic oversight, make decisions for escalations, and drive service improvements.

h) Feedback and Continuous Improvement

- The Client will have regular opportunities to provide feedback through surveys, review meetings, and direct communication with the account manager.
- Based on the feedback received, the Consulting Firm will make improvements to enhance service delivery and ensure client satisfaction.
- An annual review of the communication plan will be conducted to ensure its effectiveness and make adjustments as needed.

ANNEX 1

Standards, tools, and configurations to be used during the execution of this assignment:

1. **Industry Standards and Compliance Requirements**

   International Standards:

   a) Uptime Institute Tier Standards (Tier I-IV) – Defines availability and redundancy levels.
   b) ISO/IEC 27001 – Information security management system (ISMS) for data centres.
   c) ISO/IEC 20000 – IT service management for efficient service delivery.
   d) ISO 50001 – Energy management system for improved efficiency.
   e) ASHRAE 90.4 – Energy efficiency standard for data centre design.
   f) TIA-942 – Telecommunications infrastructure standard, covering design, redundancy, and environmental considerations.
   g) SOC 2 (Service Organization Control) – Compliance for security, availability, and processing integrity.
   h) GDPR/CCPA – Data privacy regulations for handling personal data (if applicable).
   i) NIST SP 800-53 – Security controls for federal information systems.
   j) HIPAA (if handling healthcare data) – Compliance for healthcare-related information.

2. **Essential Tools for Managed Data Centre Services**
   a) Infrastructure Monitoring and Management Tools
      - DCIM (Data Centre Infrastructure Management) Tools
      - Server and Network Monitoring Tools
      - Power and Cooling Monitoring
      - Capacity Planning Tools

   b) Security and Compliance Tools
      - Security Information and Event Management (SIEM)
      - Vulnerability Assessment Tools
      - Firewall and Intrusion Prevention
      - Access Control and Identity Management

   c) Backup and Disaster Recovery Tools
      - Backup Solutions
      - Disaster Recovery (DR)

   d) Automation and Configuration Management Tools
      - Infrastructure as Code (IaC)
      - Patch Management

   e) Performance and Cost Optimization Tools
      - Cloud Cost Management

- Performance Optimization

3. **Required Configurations for Managed Services**
   a) Network Configuration
      - Redundant Connectivity
      - Firewall Configuration
      - Load Balancing

   b) Storage Configuration
      - RAID Levels (RAID 5/6/10) for redundancy and performance.
      - SAN/NAS Configuration for distributed storage management.
      - Storage Tiering for efficient data placement (Hot, Warm, Cold).

   c) Security Configurations
      - Access Controls: Role-Based Access Control (RBAC), MFA enforcement.
      - Data Encryption: In-transit (TLS), At-rest (AES-256).
      - SIEM Logging: Centralized logging for security events.

   d) Compute Configuration
      - Virtualization Platforms
      - Resource Allocation: CPU, memory, and storage limits per workload.
      - Automation: Autoscaling and orchestration using Kubernetes, Docker.

   e) Power and Cooling Configurations
      - Power Redundancy: UPS, backup generators with automatic switchover.
      - Cooling Strategies: Hot/cold aisle containment, liquid cooling if required.
      - Environmental Monitoring: Temperature, humidity thresholds set per ASHRAE guidelines.

4. **Key Performance Indicators (KPIs) for Managed Services**
   - Availability/Uptime (99.982% for Tier 3)
   - Power Usage Effectiveness (PUE) < 1.5
   - Mean Time to Repair (MTTR)
   - Mean Time Between Failures (MTBF)
   - Data Backup Success Rate (≥ 99%)
   - Incident Response Time (within SLA)
   - Security Incident Detection Time
   - Capacity Utilization (CPU, Storage, Bandwidth)