TERMS OF REFERENCE (ToR)

Firm to Enhance Government Data Center Operational and Maintenance Capabilities

Background

The Cloud Services Division (CSD) of the GovTech Agency is executing a strategic initiative to optimize its Government Data Center (GDC) infrastructure, right-size its resources and improve the resilience of the existing legacy estate. In view of this initiative, CSD will hire a firm to enhance GDC Operational and Maintenance Capabilities to work alongside CSD teams, building on the Data Center (DC) Expert's assessment to fix capacity and resilience gaps while transferring knowledge.

Rather than duplicating prior work undertaken by the DC Expert, the deployed technical experts from the firm will work directly with the CSD team at the operational level to review and validate the DC Expert's findings, determining their direct implications for a resilient, right-sized and well-monitored data center. Through joint technical working sessions, hands-on configuration work and structured design workshops, the technical experts will work closely with the CSD team to assess and optimize the existing DC environment. The engagement will focus on developing a comprehensive understanding of the agency's current network, compute, storage, virtualization platforms, operating systems and operational capabilities. This will include identifying technical, configuration and architectural gaps, and developing and implementing practical, actionable rectification plans.

This integrated approach will ensure that the proposed design reflects the division's operational realities, aligns with established internal technical standards, and supports sustainable implementation. It will also emphasize knowledge transfer and collaboration, enabling agency teams to build the skills and understanding needed to effectively manage and evolve the optimized environment. Ultimately, this close partnership will empower the CSD team to effectively oversee the implementation and independently manage the optimized data center over the long term.

Purpose of the Assignment

The primary purpose of this assignment is to translate the baseline findings of the Data Center Assessment into validated, implemented and signed-off improvements that make the existing GDC estate right-sized, well-designed, resilient and fully monitored. Delivered primarily through intensive, on-site engagement at the

GDC, the firm will work directly alongside the CSD team to address identified infrastructure gaps, re-architect the network, harden the platform and establish capacity and performance visibility.

The Firm shall perform the following core activities on-site:

- **DC Assessment Review & Rectification:** Review the DC Expert deliverables, validate the findings on-site with the CSD team, prepare rectification plans, implement the agreed changes, and obtain CSD sign-off.
- **Resource Right-Sizing:** Assess whether existing compute, storage and network resources are allocated correctly, and right-size existing VMware workloads.
- **Network Re-architecture:** Re-design and re-configure the GDC network to best-practice designs, including segmentation, routing and route optimization, and Cisco and FortiGate firewall rules and policies.
- **DNS Redundancy & Monitoring:** Establish redundant DNS services and implement monitoring tools for capacity, performance, logs and bandwidth attacks, integrated with alerting.
- **Resilience & Hardening:** Improve the resilience of the current legacy estate, harden VMware vSphere, and add bare-metal servers for hosting containerized workloads (bare-metal container hosting).

Duration of Assignment and Level of Effort

The total duration of this assignment shall be **six (6) months** from the date of contract signing, inclusive of mobilization, on-site execution, knowledge transfer, and final sign-off of all deliverables. The firm shall mobilize its lead on-site expert within two (2) weeks of contract signing.

The engagement shall be structured around the phase-wise milestones defined under the Payment Schedule and shall follow the indicative work plan set out under Phased Deployment and Work Plan. Each phase shall be subject to CSD review and acceptance prior to progression to the subsequent phase.

The minimum on-site input for each key expert is set out in the table below. The firm shall propose its total person-day input by key expert, split between on-site and remote input.

Key expert	Phase(s)	Minimum on-site person-days
Senior Lead – System Engineering Architect	1 and 5	30 (20 + 10)
Infrastructure Engineer (mid-level)	1	20
Network and Security Specialist	2	25
Virtualization and Storage Specialist	3	25
Linux and Container Platform Specialist	4	25
Total		**125**

Remote input, including the Senior Lead's weekly reviews during Phases 2 to 4 and the firm's back-office support, is in addition to these minimums.

Extension & Renewal

The Client reserves the right to extend the contract period, either in full or in part, for up to an additional three (3) months, subject to:

- Satisfactory performance of the firm, as evidenced by CSD's acceptance of deliverables and monthly progress reports;
- Mutual written agreement between CSD and the firm on the extended scope, duration, and associated costs;
- Availability of budget and continued operational requirement; and
- Execution of a formal contract amendment prior to the expiry of the original contract period.

Any extension shall be governed by the same terms, conditions, rates, and performance obligations as the original contract, unless expressly modified in writing.

Key Methodology & Guiding Principles

The assignment follows a structured "Review – Validate – Gap Assess – Rectify – Implement – Sign-off" delivery framework. The firm will not duplicate or reproduce the previous DC Expert's work, but will build upon it to deliver implemented improvements.

The methodology addresses key technical questions at each stage:

- **Review:** What baseline conditions, capacity limits and risks were identified in the initial assessment?
- **Validate:** Are those findings still accurate given current on-site physical, configuration and logical conditions?
- **Gap Assess:** What are the specific technical, configuration and capacity gaps, and what is their operational impact?
- **Rectify:** What rectification plan, sequence, change window and rollback plan are required for each gap?
- **Implement:** How will the agreed changes be implemented jointly with CSD, and validated with CSD's existing DevOps team where workloads are affected?
- **Sign-off:** Have the agreed acceptance criteria been met, and has CSD formally signed off each rectification?

All changes to production systems shall follow CSD's change management process, with approved change windows and documented rollback.

Key Objectives

The assignment aims to translate prior data center findings into implemented operational improvements through hands-on, on-site execution at the GovTech Agency. Key objectives include:

- **On-Site Assessment & Validation:** Review the DC Expert assessment and conduct on-site technical evaluations to verify critical baseline findings, configurations and hardware conditions.
- **Gap Analysis & Rectification:** Identify specific infrastructure and configuration gaps, determine asset remediation needs (retain, upgrade or replace), and implement agreed rectifications through to sign-off.
- **Resource Right-Sizing & Capacity Planning:** Determine whether existing resources are allocated correctly, right-size existing VMware workloads, and confirm whether current capacity can support interim hosting and the deployment of monitoring tools at the GDC.
- **Network Re-architecture & Firewall Configuration:** Deliver a full network re-architecture and configuration, including segmentation, tenant isolation, routing and route optimization, and Cisco and FortiGate firewall rule and policy configuration.
- **DNS Redundancy:** Design and implement redundant, monitored DNS services.
- **Monitoring & Alerting:** Implement capacity monitoring, performance monitoring, log collection and bandwidth-attack detection, integrated with alerting.

- **Resilience & Hardening:** Improve the resilience of the legacy estate, harden VMware vSphere and ESXi.
- **Bare-Metal Capacity:** Recommend and provision bare-metal servers for running containerized workloads directly on physical hardware (bare-metal container hosting).
- **Workload Validation:** Work with DSD's existing DevOps team towards building a GDC modernization and Cloud Native Readiness platform.
- **On-Site Capacity Building & Knowledge Transfer:** Deliver continuous, embedded knowledge transfer and technical enablement to CSD staff throughout all project phases.

Baseline Materials

The baseline documentation provided by CSD, encompassing GDC facility records, infrastructure inventories, network topologies, device configurations and DC Expert deliverables, shall serve as the primary technical foundation for the assignment.

The firm shall review and map these inputs against the key optimization objectives:

- **Facility & Space:** Map current GDC space and rack utilization against current and projected IT load, including planned bare-metal servers.
- **Compute & Storage Hardware:** Audit existing asset inventories and lifecycle data to determine which servers and NetApp components can be retained, upgraded or decommissioned.
- **Network Topology & Traffic Management:** Evaluate existing network schematics, routing and firewall configurations to design best-practice segmentation, optimized routing and multi-tenant isolation.
- **Security and Backup & Replication:** Bridge identified perimeter, hardening, backup and replication gaps to strengthen protection and recoverability of critical government workloads.

Data Center Findings Validation Matrix

The firm shall establish and maintain a Data Center Findings Validation Matrix. This matrix systematically maps the DC Expert's baseline findings to on-site evidence, operational impact and required rectification across core technical domains, and tracks each item through to CSD sign-off.

Validation Classification Framework

Each finding shall be categorized under one of five explicit statuses:

- **Validated:** Confirmed through on-site inspection, configuration review and verified logs.
- **Partially Validated:** Confirmed in principle, but technical scope or conditions have changed.
- **Not Validated:** Unsupported by current on-site evidence or measurement.
- **New Finding:** Critical issue or gap identified by the firm during on-site activities.
- **Closed/Resolved:** Issue has already been remediated by CSD staff.

Domain-Aligned Findings Validation Matrix

Domain	Baseline DC Expert Finding	Validation Status	On-Site Evidence / Telemetry	Operational / Resilience Impact	Rectification Action	Priority	Sign-off
Power & Cooling Facility inside the DC Environment							
Physical Security and Access Control							
Surveillance and Environment Monitoring							
Lighting, Space and Tenancy							
Compute Infrastructure (incl. Bare-Metal							

Container Hosting)							
Storage Infrastructure (NetApp)							
Network Infrastructure							
Firewall and Perimeter Security							
DNS							
Virtualization Platform (VMware)							
Operating Systems							
Monitoring and Alerting							
Security Posture							
Backup & Replication							
Operational Maturity							

Mandatory On-Site Presence & Joint Technical Execution

The selected firm shall maintain a dedicated and continuous on-site presence at the GovTech Agency and GDC facilities throughout the engagement period. The firm shall function as an embedded technical partner, working directly alongside the CSD team through day-to-day co-working, on-site assessments, configuration and implementation work, technical working sessions and design workshops. This approach shall ensure

continuous knowledge transfer, timely validation of findings, joint decision-making and close alignment with CSD's operational and technical requirements.

The firm's financial engagement model shall be structured around monthly payment disbursements, with each monthly invoice supported by verified on-site attendance, joint execution and activity logs, progress against agreed work plans shared with the CSD team, and evidence of completed or progressing deliverables. The CSD team shall review and validate the firms monthly activities and deliverable progress prior to payment.

Expert Deployment Criteria

- **Lead Technical Presence:** The firm shall deploy at least one dedicated senior technical expert physically on-site throughout all critical phases of the assignment.
- **Direct CSD Integration:** The expert shall sit and work directly alongside CSD's system and network personnel to co-execute inspections, configuration changes and implementation activities.
- **Support Framework:** Specialized remote engineers may provide back-office support, but shall not replace the mandatory primary on-site lead.
- **Access & Change Control:** All access to GDC systems shall follow CSD's access, security and change management procedures. The firm shall sign a non-disclosure agreement.

Monthly Payment Mandate

Monthly payment disbursements shall be contingent upon the fulfilment of the following conditions:

- Verified On-Site Engagement: Confirmation of the agreed monthly physical on-site person-days, substantiated by attendance records and timesheets duly signed and endorsed by the designated CSD representative.
- Monthly Progress Reporting: Submission of a comprehensive monthly progress report documenting joint activities completed, configuration and infrastructure changes implemented, and the current status of the Data Center Findings Validation Matrix.

On-Site Data Center Validation & Technical Assessment

The firm, working directly alongside the CSD team, shall validate the previous DC Expert's findings and implement the agreed rectifications across the following core domains.

Facility and Physical Infrastructure

The firm shall perform physical on-site audits with the CSD team to evaluate:

- Data center rack availability, rack utilization and physical equipment layouts.
- Cable management and physical access security.
- **Target Assessment:** Determine whether current space and rack capacity can support existing equipment, planned bare-metal servers and future growth in terms of power and cooling workload.

Network Infrastructure, Re-architecture & Configuration

The firm shall evaluate and re-architect core network switches, routing topologies and edge appliances:

- Core, distribution, access and top-of-rack switching, server NIC connectivity and link redundancy against best-practice data center designs.
- Segmentation using VLANs/VRFs for management, production, storage, backup and DMZ networks.
- Static and dynamic routing, route summarization and route optimization, including removal of suboptimal or asymmetric paths.
- Link aggregation (LACP), redundant uplinks and dual-homing.
- Uplink bandwidth utilization, WAN/Internet connectivity and ISP redundancy.
- **Target Assessment:** Deliver a full network re-architecture and configuration of Cisco routers and switches, with updated physical and logical network diagrams.

Firewall Rules, Routing & Policies

The firm shall audit and reconfigure Cisco and FortiGate firewalls:

- Existing rule bases, NAT, tenant isolation, routing and zone design.
- Unused, shadowed, redundant and over-permissive (any-any) rules.
- IPS, application control and DoS/bandwidth-attack protection features available on the platforms.
- Firewall throughput and session capacity against current and projected traffic.
- **Target Assessment:** Deliver a cleaned-up, least-privilege firewall policy base aligned with the new segmentation design, and a rule review and change process with CSD.

DNS Redundancy

- Current DNS architecture, zones, dependencies and single points of failure.
- **Target Assessment:** Design and implement redundant DNS services across separate hosts and failure domains, with service health and query monitoring integrated into alerting.

Compute Resources, Server Hardware & Bare-Metal

The firm shall audit server inventories and physical resource margins:

- Physical server hardware, CPU core counts, memory capacity, baseline utilization, firmware levels and lifecycle status.
- Bare-metal container hosting requirements: suitable physical servers, host operating system and container runtime, sizing, and network and storage connectivity.
- Vendor hardware support contracts and warranty status.
- **Target Assessment:** Determine whether existing hardware can be retained, upgraded or must be replaced, and recommend and provision bare-metal servers for container hosting.

Storage Infrastructure (NetApp)

The firm shall validate storage arrays and performance metrics:

- Capacity, utilization, aggregate and volume layout, and orphaned or unused volumes.
- Performance profiles: IOPS, latency (ms), throughput (MB/s) and queue depth under load.
- Controller redundancy, multipathing (MPIO), snapshot policies, replication, backup integration and lifecycle status.
- **Target Assessment:** Implement storage right-sizing, tiering and clean-up, and confirm headroom for current and planned workloads.

Hypervisor & Operating Systems (VMware vSphere 7 and 8)

- vCenter and ESXi cluster design, HA/DRS configuration, resource pools, hypervisor overhead and host redundancy.
- vSphere version alignment and upgrade requirements.
- Host and guest operating system baselines and patch levels.
- **Target Assessment:** Harden VMware vSphere and ESXi to vendor security configuration guidelines and define OS hardening standards.

Data Center Resilience & Failure Domain Assessment

Working directly with the CSD team, the firm shall assess and improve the operational resilience of the existing legacy estate, and identify single points of failure (SPOFs), operational weaknesses and resilience gaps across the critical operational vectors below. The firm shall translate the DC Expert's findings into

actionable operational and technical improvements and support their implementation, including infrastructure operations, monitoring, maintenance, capacity management, backup and recovery, redundancy, failover and incident management. All gaps shall be prioritized by service criticality, operational risk, implementation feasibility and available resources, with clear ownership, timelines and measurable outcomes.

SPOF Assessment Framework

- **Network:** Address single top-of-rack switches, non-LACP uplinks, single-homed edge routers and non-redundant routing paths.
- **Compute:** Address non-clustered hypervisors and hosts without HA capacity.
- **Storage:** Address single-controller arrays, non-RAID local drives and single-path Fibre Channel/iSCfirm connectivity without MPIO.
- **Internet Connectivity:** Address single ISP fiber entry points and common ducting, single BGP peering and single edge NAT/firewall hardware.
- **Security:** Address single perimeter firewalls and non-HA identity and management services.
- **DNS:** Address single DNS servers and shared failure domains for name resolution.
- **Backup:** Address single-site backup targets, unencrypted backups and the absence of immutable or air-gapped copies.

The firm shall not limit its engagement to documenting these findings. All agreed findings shall be tracked through a formal remediation register, with progress reviewed jointly with CSD until closure. Where full remediation cannot be immediately implemented due to technical, operational or budgetary constraints, the firm shall provide risk-based interim controls and a clearly defined remediation roadmap.

Security Validation & Hardening

The firm shall validate the DC Expert's security findings and implement hardening across the infrastructure layers:

- **Perimeter & Network Security:** Evaluate Cisco and FortiGate firewall throughput, network segmentation (VLANs, VRFs), IDS/IPS and DoS/bandwidth-attack protection.
- **Identity & Access Management (IAM):** Review centralized identity stores (Active Directory, LDAP), privileged access for root/admin accounts, and multi-factor authentication across infrastructure management interfaces.

- **VMware Hardening:** Apply vendor security configuration guidelines to vCenter and ESXi, including lockdown mode, SSH, local accounts, certificates and logging.
- **Vulnerability & Log Monitoring:** Audit vulnerability scanning schedules, patching lifecycles, host-level server hardening (CIS benchmarks), and centralized log collection from firewalls, network devices, ESXi/vCenter, storage and servers.
- **Physical Security:** Inspect biometric/card access controls, CCTV coverage and retention, rack lock integrity and visitor log auditing within the server halls.

Backup & Replication

Based on the DC Expert's review, the firm shall evaluate, audit and validate the current environment across the following domains:

- **Backup Architecture:** Assess existing backup infrastructure, storage targets, retention schedules, and encryption at rest and in transit.
- **Replication Strategy:** Evaluate current NetApp, VM-level and database-native replication between the primary GDC and the backup site.

Capacity Planning, Right-Sizing & Monitoring Assessment

Based on the DC Expert's findings and the firm's validation, the firm shall determine whether existing GDC resources are allocated correctly and whether current capacity can support interim hosting requirements and the deployment of monitoring tools at the GDC.

The assessment shall cover:

Domain	Assessment
Compute	Utilization and right-sizing
Storage	Utilization and right-sizing
Network	Bandwidth utilization and headroom
Virtualization (VMware)	Cluster capacity and right-sizing
Monitoring	Coverage and gaps
Alerting	Integration and escalation

Operations	Capacity management maturity
Skills	Readiness

The firm shall provide an overall capacity rating and define the additional capacity required, if any.

Right-Sizing of Existing VMware Workloads

- **Data Collection:** Collect utilization data for all VMware workloads (CPU, memory, storage and network) over a representative period.
- **Analysis:** Identify over-provisioned, under-provisioned, idle and zombie VMs.
- **Workload Validation:** Work with CSD's existing DevOps team and application owners to validate existing workloads before any change.
- **Implementation:** Implement agreed right-sizing changes and report reclaimed capacity.

Monitoring, Logging & Alerting

- **Capacity Monitoring:** Track compute, storage and network utilization against agreed thresholds.
- **Performance Monitoring:** Monitor host, VM, storage latency/IOPS and network performance.
- **Hardware Health:** Monitor servers, NetApp and network devices.
- **Traffic & Bandwidth-Attack Detection:** Monitor bandwidth and traffic anomalies, including volumetric attacks.
- **Log Collection:** Centralize logs from firewalls, network devices, ESXi/vCenter, storage and servers.
- **Alerting Integration:** Integrate alerts with CSD's notification channels, with agreed thresholds and escalation, and build dashboards for capacity, performance and service health.

Deliverables Statement of Work

The firm shall produce and submit the following formal deliverables to CSD during the engagement. Each deliverable shall be reviewed and signed off by CSD.

- **Review of Existing Data Center Expert Assessment:** Formal verification report and context analysis of the pre-existing data center documentation.
- **Data Center Findings Validation Matrix:** Tracing matrix validating prior findings against current physical and logical realities, maintained until sign-off.

- **Rectification Plans:** Per-domain plans covering technical changes, sequence, change windows, rollback, testing and acceptance criteria.
- **Updated Data Center Assessment:** Current-state audit covering physical infrastructure, lifecycle status and operational health.
- **Network Re-architecture Design & Implementation Report:** Target design, segmentation, routing and route optimization, as-built diagrams and configurations.
- **Firewall Policy Review & Configuration Report:** Rule clean-up, new policy base, zone design and as-built Cisco and FortiGate configurations.
- **DNS Redundancy Implementation Report:** Design, configuration and failover test results.
- **Compute, Storage & Bare-Metal Assessment:** Hardware lifecycle, retain/upgrade/replace recommendations, and bare-metal container hosting sizing and provisioning.
- **VMware & OS Hardening Report:** Applied hardening baseline, exceptions and compliance status.
- **Right-Sizing Report:** Workload-level findings validated with the DevOps team, changes made and capacity reclaimed.
- **Capacity Plan:** Current utilization, sufficiency for interim hosting and monitoring tools, thresholds and growth projections.
- **Monitoring & Alerting Implementation Report:** Tools deployed, log sources, dashboards, thresholds and alert integration.
- **Security Assessment:** Gap analysis covering physical security, segmentation, perimeter defenses, IAM and hardening.
- **Backup:** Backup success rates, replication, RPO/RTO metrics and restore test results.
- **Resilience Improvement Report:** SPOFs removed, interim controls and remaining remediation roadmap.
- **Runbooks, SOPs & As-Built Documentation:** Operational procedures for all implemented changes.
- **Knowledge Transfer & Final Report:** Training delivered, skills handed over, final status and sign-off.

Consultancy Requirements

The Integrator shall have proven experience in delivering data center infrastructure integration and optimization projects of comparable size and complexity (in terms of the number of servers, virtual machines, storage, network and security infrastructure), preferably for government or large enterprise clients. The firm shall propose, at minimum, the following five key experts:

1. **Senior Lead – System Engineering Architect (on site in Phases 1 and 5):**
    a. A minimum of twelve (12) years of experience in data center infrastructure, including at least five (5) years leading infrastructure optimization or integration projects.
    b. The expert shall demonstrate:
        i. Hands-on experience with VMware vSphere 7 and 8, vCenter, ESXi, cluster management, and virtualization capacity planning.
        ii. Experience with enterprise server hardware, NetApp storage, operating systems, and infrastructure lifecycle management.
        iii. Experience with infrastructure hardening, monitoring, automation, backup, and disaster recovery.
        iv. Ability to assess resource utilization and implement workload right-sizing.
        v. Experience with data center power and cooling assessments, including interpreting equipment power requirements, utilization data, cooling constraints, and available capacity, or demonstrable experience coordinating these assessments with qualified facility engineers.
        vi. Experience preparing technical designs, implementation plans, operational documentation, and knowledge-transfer materials.
    c. **Certification Requirement:**
        i. A valid VMware Certified Professional (VCP) certification relevant to data center virtualization or the proposed VMware environment.
        ii. Additional relevant certifications, such as VMware Certified Advanced Professional (VCAP), NetApp Certified Data Administrator (NCDA), Certified Kubernetes Administrator (CKA), or Red Hat Certified Engineer (RHCE), if any.

2. **Infrastructure Engineer (mid-level, on site in Phase 1):**
    a. A minimum of four (4) years of experience in data center operations or infrastructure support, covering servers, virtualization and networking.
    b. The expert shall demonstrate:
        i. Infrastructure discovery, inventory and configuration data collection.
        ii. Preparation of network diagrams, inventories and technical documentation.
        iii. Support to senior engineers in assessment and validation activities.
    c. Certification Requirement:
        i. None mandatory; Cisco Certified Network Associate (CCNA) or VMware Certified Technical Associate (VCTA), preferred.

3. **Network and Security Specialist (on site in Phase 2):**
    a. A minimum of seven (7) years of hands-on experience in enterprise or data center networking and security.
    b. The expert shall demonstrate:
        i. Hands-on experience with Cisco routers, switches, enterprise networking, VLANs/VRFs, routing, redundancy, and network troubleshooting.
        ii. Experience with Cisco and Fortinet FortiGate firewall configuration, security policies, NAT, and network segmentation/tenant isolation.
        iii. Knowledge of network monitoring, traffic analysis, access controls, and relevant security practices.
        iv. Experience developing and maintaining network diagrams, configuration records, and implementation documentation.
    c. **Certifications Requirement:**
        i. Valid Cisco Certified Network Associate (CCNA).
        ii. Valid Cisco Certified Network Professional (CCNP).
        iii. Valid Fortinet NSE 4 (FortiGate) certification or higher.

4. **Virtualization and Storage Specialist (on site in Phase 3):**
    a. A minimum of seven (7) years of hands-on experience with VMware virtualization and enterprise storage.
    b. The expert shall demonstrate:
        i. Hands-on experience with VMware vSphere 7 and 8, vCenter, ESXi, HA/DRS cluster design, and hardening to vendor security configuration guidelines.
        ii. Hands-on experience with NetApp ONTAP storage, including aggregate and volume design, snapshots, replication and multipathing.
        iii. Experience with enterprise backup platforms, including job design, immutable or air-gapped copies, and restore testing.
        iv. Experience with VMware workload right-sizing and virtualization capacity planning.
    c. Certification Requirement:
        i. A valid VMware Certified Professional – Data Center Virtualization (VCP-DCV) certification.
        ii. NetApp Certified Data Administrator (NCDA) and a backup platform certification (e.g., Veeam Certified Engineer), preferred.

5. **Linux and Container Platform Specialist (on site in Phase 4):**

a. A minimum of seven (7) years of Linux systems administration, including at least three (3) years with container platforms.

b. The expert shall demonstrate:

   i. Linux server hardening against CIS benchmarks, and patch and baseline management.

   ii. Deploying and operating Kubernetes and container runtimes on bare-metal servers, including network and persistent storage integration.

   iii. Deploying open-source monitoring, logging and alerting stacks (e.g., Prometheus and Grafana, Zabbix, or OpenSearch) and integrating alerts with notification channels.

   iv. Infrastructure automation and configuration management (e.g., Ansible).

c. Certification Requirement:

   i. A valid Certified Kubernetes Administrator (CKA) or Red Hat Certified Engineer (RHCE) certification.

The firm shall submit CVs, certifications and references for each key expert. Key experts shall not be replaced without CSD's written approval. The CVs of all five key experts shall be evaluated and scored.

Evaluation of Technical Proposals

The Evaluation Committee shall evaluate the Technical Proposals on the basis of their responsiveness to this Terms of Reference, applying the evaluation criteria, sub-criteria and points system set out below. Each responsive Proposal shall be awarded a technical score (St).

A Proposal shall be rejected at this stage if:

- It does not respond to important aspects of this Terms of Reference, particularly the scope of work, deliverables and key expert requirements; or
- It fails to achieve the minimum technical score indicated in the Tender Notice.

Overall Evaluation Weighting

The final evaluation of Proposals shall be based on a combined technical and financial score, weighted as follows:

Evaluation Component	Weight
Technical Proposal (St)	80%
Financial Proposal (Sf)	20%

Total	100%

The weights given to the Technical and Financial Proposals are:

T = 0.80, and

P = 0.20

The Financial Proposal score (Sf) of each technically qualified Proposal shall be computed using the following formula:

Sf = 100 × Fm / F

in which **Sf** is the financial score, **Fm** is the lowest price and **F** the price of the proposal under consideration.

The lowest-priced technically qualified Proposal shall therefore receive a financial score of 100, and higher-priced Proposals shall receive proportionally lower scores.

The combined score (S) of each Proposal shall be computed as:

S = (St × T) + (Sf × P) = (St × 0.80) + (Sf × 0.20)

The contract shall be awarded to the Bidder with the highest combined score, subject to successful contract negotiations.

Evaluation Criteria and Points Allocation

The criteria, sub-criteria and points system for the evaluation of Technical Proposals are as follows:

#	Evaluation Criterion / Sub-criterion	Points
i	**Specific Experience of the Consultant Relevant to the Assignment**	**5**
ii	**Adequacy of the Proposed Work Plan and Methodology in responding to the Terms of Reference**	**15**
ii-a	Technical Approach and Methodology	12
ii-b	Work Plan	3
iii	**Key Professional Staff Qualifications and Competence for the Assignment**	**80**
iii-a	General Qualification	16
iii-b	Adequacy for the Assignment	64
	Total Points	**100**

The minimum technical score required to pass is 75 points. Proposals scoring below this threshold shall not proceed to the financial evaluation stage.