Government IT Services Transformation Initiative (GITS)

Annex A – Draft Terms of Reference for Market Consultation

Request for Expression of Interest / Market Consultation Package

for the Procurement of Workplace and Workstation as a Service (WaaS), Virtual Desktop as a Service (DaaS), Managed Print as a Service (PraaS), Managed Network as a Service (NaaS), Unified Communications as a Service (UCaaS), Managed Wireless LAN as a Service (WLANaaS), and Managed Meeting Room and Collaboration Equipment as a Service on a lease/service basis, including Acquisition, Deployment, Management and Support

Item	Indicative position for consultation
Document status	Working draft issued for REOI market consultation only
REOI organizer / market consultation coordinator	Information Systems Agency of Armenia (ISAA), on behalf of the Government of the Republic of Armenia
Expected pilot contracting authority	Prime Minister's Office of the Republic of Armenia
Future procurement approach	Expected competitive procurement procedure, OPEN TENDER
Commercial structure under consultation	One Prime Contractor / Lead Member with end-to-end accountability; consortium, JV, subcontracting, OEM, distributor, leasing and financing partner structures permitted subject to full accountability
Indicative pilot baseline	Approximately 1,200–1,300 end users, plus related service-tower quantities to be validated
Indicative contract term under consultation	36 months, with possible extension and priced expansion options, subject to legal and budgetary approval
Submission language for market feedback	English

Consultation status

This Draft TOR is not a tender document and does not request binding technical or financial offers. It is issued to obtain structured market feedback on scope, feasibility, service delivery model, technical and conformity requirements, SLA/KPI assumptions, commercial structure, implementation dependencies, risk allocation, and contract-management arrangements.

Purpose and Status of this Draft TOR

This Draft Terms of Reference forms Annex A to the GITS REOI market consultation package. Its purpose is to present the current working draft of the service, operational, technical, governance, security, commercial and transition requirements that may inform a future procurement process.

Interested parties are invited to review this Draft TOR and provide structured comments through the official TOR Comment Matrix and related response forms. Comments should identify requirements that are clear, unclear, proportionate, restrictive, costly, operationally challenging, not feasible, or capable of improvement through alternative wording or market-standard delivery models.

Important interpretation rule

References in this Draft TOR to “shall”, “must”, “Contractor”, “Bidder”, “proposal”, “Contract”, “acceptance”, “service credits” or similar future-procurement terms describe contemplated future procurement and contract requirements. They do not create obligations under the REOI and do not constitute a request for binding offers.

1. Background

The Government of the Republic of Armenia is implementing the **Government IT Service Transformation (GITS) project** as a strategic initiative to modernize and standardize the delivery of end-user information technology services across public authorities. The GITS project is intended to establish a more uniform, secure, service-oriented, and cost-effective operating model for end-user computing environments used by ministries and other state bodies.

At present, end-user devices and related support services are procured, deployed, and managed through multiple separate institutional arrangements across government. This has resulted in fragmented technical standards, uneven lifecycle management, inconsistent support quality, varying refresh practices, increased administrative burden, limited interoperability, and reduced visibility over aggregate costs, operational performance, and service-related risks. The current model also places substantial operational responsibility on individual public bodies for matters such as configuration, deployment, maintenance, support, replacement planning, sanitization, and disposal, thereby reducing standardization and increasing complexity in day-to-day administration.

Through the GITS project, the Government seeks to move from a predominantly equipment-purchase and ownership model to a **managed service model** under which end-user computing services are delivered in accordance with defined service classes, standardized technical baselines, measurable service levels, lifecycle accountability, and periodic service payments. This model is intended to strengthen cybersecurity governance, improve budget predictability, strengthen continuity of operations, reduce fragmentation, support enforceable service performance, and ensure that technology services provided to public servants are better aligned with their functional roles and operational requirements.

The GITS project further aims to introduce a structured end-user service framework comprising defined service classes and configuration categories designed to reflect differences in user profiles, mobility needs, performance requirements, and operational environments. Under this framework, end-user computing services are to be delivered not merely as isolated equipment purchases, but as integrated service packages encompassing, as applicable, acquisition, logistics, configuration, installation, enrolment, asset registration, support, maintenance, replacement, refresh, return, data sanitization, monitoring and reporting, and transition management, all subject to contractual performance requirements.

In this context, the **Prime Minister's Office of the Republic of Armenia**, acting as the Contracting Authority for the pilot phase of the GITS project, is launching an **open tender** for the establishment of a **single integrated public contract** for the approved pilot scope. The contract is intended to support the acquisition, deployment, management, support, lifecycle operation, and orderly transition of end-user computing services for the participating entities covered by the pilot. The procurement is structured as a **single lot** in order to ensure unified contractual accountability, consistent service

governance, integrated service management, and a coherent implementation model across the pilot environment.

The Contracting Authority requires that the successful Bidder act as the **Prime Contractor** and assume full end-to-end responsibility for contract performance. Participation through a consortium, joint venture, or other permitted association of economic operators shall be allowed only on the condition that such Bidder designates a **Lead Member** authorized to act on behalf of the consortium and to bear, jointly and severally with the other members, full contractual responsibility for the performance of all obligations under the Contract. Any use of subcontractors, service partners, manufacturers, distributors, lessors, or other delivery partners shall not relieve the Prime Contractor of full responsibility for service delivery, compliance, reporting, security, transition, or performance against the Contract.

The pilot procurement under the GITS project is intended to establish a service model that is operationally viable for immediate implementation and sufficiently structured to support later scaling, subject to applicable legal, institutional, financial, and policy decisions. The Government therefore seeks a solution that is not only technically compliant, but also operationally mature, scalable, supportable, auditable, secure, and suitable for sustained use in the public sector.

Separate procurement boundary: For the avoidance of doubt, this procurement concerns end-user computing and related managed services only, as expressly described in the Request for Proposal and its Annexes. **Microsoft products, licenses, subscriptions, tenant services, and Microsoft-related support services are outside the scope of this procurement and shall be procured separately under a different procurement procedure.** Any references in this tender to interoperability, compatibility, integration readiness, endpoint dependencies, identity dependencies, or coexistence requirements shall be interpreted solely as boundary and interface requirements and shall not be construed as including Microsoft procurement, Microsoft subscription services, or Microsoft support within the scope of this Contract.

Likewise, unless expressly stated otherwise in the Technical Specifications or other Annexes, **data center services, core hosting services, and unrelated central platform services are outside the scope of this solicitation**.

The Contracting Authority accordingly invites proposals from qualified Bidders capable of delivering the required GITS pilot services in a lawful, secure, efficient, and public-sector-appropriate manner, consistent with the objectives of the GITS project and the requirements set out in this Request for Proposal, the Terms of Reference, the Service Level requirements, the Security Schedule, and the Draft Contract.

2. Objectives

The overall objective of this procurement is to establish, through the pilot phase of the Government IT Service Transformation (GITS) project, a standardized, secure, service-oriented, and operationally

sustainable framework for the delivery of end-user computing and related managed services for the **Prime Minister's Office of the Republic of Armenia**.

More specifically, the Contracting Authority seeks to replace fragmented and asset-centric end-user computing arrangements with an integrated managed service model under which the successful Contractor assumes defined responsibilities for the acquisition, ordering, logistics, configuration, enrolment, deployment, support, maintenance, break/fix, replacement, refresh, return, sanitization, monitoring, reporting, and orderly transition of end-user computing services, in accordance with the Contract.

A central objective of the GITS pilot is to implement a structured end-user service model based on **eleven defined service classes** and common technical baselines. This model is intended to ensure that users of the Prime Minister's Office receive end-user computing services appropriate to their functional roles, mobility requirements, performance needs, and operational environments, while maintaining common standards for manageability, interoperability, lifecycle control, supportability, and security.

This procurement also supports a transition from a predominantly equipment-purchase and ownership model to a **managed service and operational expenditure model**. Under the service model, the Contractor assumes defined lifecycle and operational responsibilities under a comprehensive service contract governed by performance obligations, security requirements, reporting duties, and contractual accountability. This approach is intended to improve budget predictability, reduce irregular capital investment needs, strengthen operational continuity, and enable more disciplined management of service quality, risk, and cost.

The service model is further intended to provide greater flexibility than a traditional equipment-purchase approach. Subject to the Contract and the applicable change-control mechanism, the Prime Minister's Office should be able to increase, decrease, redeploy, replace, or otherwise adjust service volumes in accordance with actual operational needs, staffing changes, restructuring, or approved project requirements, without the delays and inefficiencies associated with repeated asset procurement cycles.

Accordingly, the objectives of this procurement are to:

a) establish a unified and coherent service delivery model for end-user computing services within the approved pilot scope, under a single integrated contract with one Prime Contractor responsible for end-to-end performance;

b) implement a structured service-class framework that aligns end-user computing services with actual user roles, operational requirements, mobility needs, and performance demands;

c) introduce a managed service model under which the Contractor assumes defined lifecycle responsibilities for end-user computing services, including acquisition, staging, deployment, support, maintenance, break/fix, replacement, refresh, return, and disposition, except where otherwise expressly stated in the Contract;

d) improve service consistency, standardization, interoperability, and lifecycle control through common service standards, configuration baselines, support processes, and reporting arrangements;

e) strengthen **cybersecurity governance, cybersecurity management, and operational cyber resilience** by ensuring that end-user computing services are delivered in accordance with defined security requirements, controlled configurations, patching and vulnerability-management obligations, access-control requirements, asset accountability measures, incident handling requirements, logging and monitoring obligations, and auditable service processes;

f) embed cybersecurity into the operating model of the service, including device provisioning, endpoint hardening, policy enforcement, security updates, threat and incident escalation interfaces, breach notification, service continuity, and secure end-of-life handling of devices and data-bearing components;

g) improve budget predictability and whole-of-life cost management by establishing a service-based commercial model under which the Prime Minister's Office pays for services actually deployed and in productive use, rather than bearing the full upfront cost and lifecycle risk of owned end-user hardware;

h) reduce ongoing operational, service-delivery, and security risks by assigning clearly defined lifecycle, support, security, and performance responsibilities to the Contractor under enforceable contractual terms;

i) ensure that the Prime Minister's Office does not pay for devices or service units that are not deployed and in service, so that where a user departs, a position is abolished, or a device is no longer required and is not redeployed, the corresponding service charge may cease in accordance with the pricing model, the Contract, and the applicable asset return and service adjustment procedures;

j) ensure that all equipment and associated end-user service components provided through the programme are subject to an ongoing refresh cycle of **three (3) years**, unless otherwise expressly stated for a specific service class or approved through the Contract's change-control mechanism

k) retain Government and Contracting Authority oversight over standards, policies, governance arrangements, cybersecurity requirements, management processes, reporting requirements, acceptance controls, and change-control decisions, while assigning day-to-day service delivery obligations to the Contractor;

l) ensure continuity of operations through effective transition-in arrangements, controlled rollout planning, service stabilization, operational support, cybersecurity incident readiness, and defined transition-out and reversibility obligations at the end of the Contract or upon partial service termination; and

m) establish, through the pilot implemented for the Prime Minister's Office, a practical and evidence-based service model capable of informing future scaling of the GITS project, subject to subsequent legal, policy, institutional, and budgetary decisions.

The purpose of this Request for Proposal is therefore to solicit proposals from qualified Bidders whose solutions align with the Government's forward-looking service transformation strategy and who can demonstrate the capacity to deliver the required services for the **Prime Minister's Office** in a manner consistent with the operational, technical, performance, security, governance, and commercial requirements set out in the procurement documents.

In furtherance of the above objectives, the Contracting Authority expects and assumes, for the purposes of this RFP, that:

2.1 this RFP is a solicitation for **services**, and the Contracting Authority intends to award a **single integrated contract** to one successful Bidder acting as Prime Contractor, on the basis of the proposal determined to be most advantageous in accordance with the evaluation methodology stated in the procurement documents;

2.2 the preferred solution shall demonstrate value for money through a combination of whole-life cost efficiency, service quality, technical suitability, delivery capability, operational maturity, cybersecurity capability, relevant experience, and reduced ongoing operating risk;

2.3 the Contractor shall provide an end-to-end managed service solution, whether directly or through approved consortium members, subcontractors, or partners, without prejudice to the Prime Contractor's full responsibility for contract performance;

2.4 the service model shall be based on actual deployment and actual service use, in accordance with the pricing schedules and asset/account management rules provided under the Contract;

2.5 the Prime Minister's Office shall retain strategic and operational oversight over service standards, governance arrangements, cybersecurity requirements, management processes, policies, and approval mechanisms, while the Contractor shall remain responsible for day-to-day service delivery and lifecycle performance within the scope of the Contract; and

2.6 proposals shall clearly demonstrate how the Bidder's solution responds to the GITS pilot objectives of standardization, lifecycle accountability, cybersecurity governance, service performance, budget predictability, and long-term operational suitability for the Prime Minister's Office.

For the avoidance of doubt, the objectives of this procurement relate only to the end-user computing and related managed services expressly described in the procurement documents for the **Prime Minister's Office**. They do not extend to the procurement of Microsoft products, licenses, subscriptions, tenant services, or Microsoft-related support services, which shall be procured separately under a different procurement procedure. Nor do they extend, unless expressly stated otherwise, to data center services, core hosting services, or unrelated central platform services.

3. Scope of Services

The scope of services under this procurement shall comprise the provision of an integrated managed service arrangement covering approved end-user computing equipment and other approved network-connected technology equipment, together with the related deployment, configuration, support, maintenance, refresh, replacement, return, and transition services expressly selected in the Procurement Summary Tables and governed by the Technical Specifications, Conformity Tables, Service Level requirements, Security Schedule, and Contract.

The scope is intended to cover the principal categories of technology equipment connected to the operational environment under the approved pilot, with end-user workstation and desktop computing services constituting the primary scope and managed network equipment services constituting the second principal component. Additional equipment categories may be included where expressly selected in the Procurement Summary Tables.

3.1 Core Scope Categories

The following categories shall constitute the principal and mandatory scope of the procurement:

No.	Service tower	Abbreviation	Scope orientation
1	Workplace and Workstation as a Service	WaaS	Managed workplace/workstation devices, accessories, endpoint lifecycle, deployment, support, replacement, refresh, secure return and service reporting.
2	Virtual Desktop as a Service	DaaS	Virtual desktop service profiles, including VDI where applicable, for selected user groups and operating models.
3	Managed Print as a Service / Print as a Service	PraaS	Managed print device fleet, secure print functions, consumables model where applicable, meter/usage reporting, maintenance and replacement.
4	Managed Network as a Service	NaaS	Managed switching, routing, firewall, SD-WAN, network security and related infrastructure equipment services.
5	Unified Communications as a Service, including Managed Voice and SIP Telephony	UCaaS	Managed voice, SIP telephony, telephony devices and related communications service components within the approved boundary.
6	Managed Wireless LAN as a Service / WiFi as a Service	WLANaaS / WiFi as a Service	Wireless LAN planning, AP lifecycle, controller/management model, monitoring, security, coverage and support.
7	Managed Meeting Room and Collaboration Equipment as a Service	Meeting Room / Collaboration Equipment as a Service	Managed meeting room, conferencing and collaboration equipment, support, maintenance, replacement, monitoring and service reporting.

3.1.1 End-User Workstation and Desktop Computing Services, WaaS/DaaS

The Contractor shall provide managed end-user workstation and desktop computing services under the approved service-class framework. This shall constitute the primary scope of the procurement.

The end-user computing service model is structured through defined service classes covering, as applicable, baseline productivity users, mobile users, performance-oriented users, tablet-based mobility use cases, cloud-centric user profiles, Desktop-as-a-Service, and Virtual Desktop Infrastructure profiles.

The Contractor shall respond to each configuration category required by the procurement documents and, where a category is requested, shall respond to all mandatory configurations within that category.

The end-user computing scope shall include, as applicable to the selected service classes and quantities:

a) workstation devices and related endpoint units;

b) monitors, docking stations, keyboards, mice, chargers, and other approved accessories;

c) device preparation, staging, configuration, enrolment, and deployment;

d) maintenance, break/fix, replacement, and refresh; and

e) redeployment, return, and end-of-service handling.

All workstation and desktop classes shall be governed by the applicable Conformity Tables. The specifications set out in those tables shall be treated as minimum requirements unless expressly stated otherwise. Equivalent or better alternatives may be proposed only where permitted by the procurement documents and where full equivalence or superiority is clearly demonstrated.

3.1.2 Managed Print Services, PraaS

Where selected, the Contractor shall provide managed services for approved network-connected printing equipment, including printers and multifunction devices.

This optional scope may include, as applicable:

a) provision of approved print devices;

b) installation and commissioning;

c) consumables supply and replenishment;

d) maintenance, repair, and replacement;

e) usage monitoring and print-service reporting; and

f) return and end-of-service handling.

3.1.3 Managed Network Equipment Services, NaaS

The Contractor shall provide managed services for approved network equipment supporting the operational environment covered by this procurement. This shall constitute the second principal component of the scope.

The managed network equipment scope shall include, as applicable to the selected categories and quantities:

a) L2 switches;

b) L3 switches;

c) routers;

d) Wi-Fi access points;

e) network firewalls, including NGFW and SD-WAN appliances; and

f) other approved network-connected infrastructure devices expressly included in the procurement documents.

The Contractor shall provide, as applicable:

a) provision and installation of approved network equipment;

b) commissioning and baseline configuration;

c) support, maintenance, repair, and replacement;

d) firmware and software lifecycle management;

e) monitoring and operational support; and

f) secure decommissioning, return, and end-of-service handling.

3.1.4 Unified Communications as a Service, including Managed VoIP and Conference Equipment Services, UCaaS

Where selected, the Contractor shall provide managed services for approved VoIP, IP telephony, and conference-room equipment connected to the relevant operational environment.

This optional scope may include, as applicable:

a) provision of approved VoIP and conference equipment;

b) installation, configuration, and commissioning;

c) maintenance, repair, replacement, and support;

d) device monitoring, inventory control, and service reporting; and

e) return and end-of-service handling.

3.1.5 Managed Wireless LAN as a Service, WLANaaS / WiFi as a Service

WLANaaS covers managed wireless LAN services, including approved wireless access points and the management, monitoring, security, support and lifecycle activities needed to deliver reliable wireless connectivity in the pilot environment.

a) wireless planning inputs, site survey or RF validation where required;

b) provision, installation, configuration and commissioning of approved wireless access points and related management components;

c) coverage, capacity, authentication, segmentation and wireless security requirements as defined in the conformity tables and future technical annexes;

d) monitoring, firmware lifecycle management, incident handling, configuration backup and reporting;

e) replacement, refresh, secure decommissioning and transition-out support.

3.1.6 Managed Meeting Room and Collaboration Equipment as a Service

Managed Meeting Room and Collaboration Equipment as a Service covers approved meeting-room, video-conferencing and collaboration equipment provided and supported as managed service components. The service is intended to ensure usability, lifecycle accountability, preventive maintenance, incident response, replacement and reporting for room-based collaboration environments.

a) provision, installation, configuration and commissioning of approved meeting room and collaboration equipment;

b) support for displays, cameras, microphones, speakers, control panels, room peripherals and related approved components;

c) preventive maintenance, readiness checks, replacement coordination and incident support;

d) inventory, location and configuration records for each room or device set;

e) usage, incident and availability reporting where technically supported;

f) secure return, decommissioning, handover documentation and transition-out support.

3.2 Procurement Summary Tables and Conformity Tables

The final contractual scope shall be determined by:

a) the service categories described in this Section;

b) the selected classes, categories, and quantities recorded in the Procurement Summary Tables;

c) the applicable Conformity Tables; and

d) the related technical, service, and commercial annexes.

Prior to contract signature, the Contracting Authority shall select the specific classes of equipment and services to be procured from the Conformity Tables, and the selected items shall be recorded in the Procurement Summary Tables as binding obligations of the Contractor. All quantities, delivery schedules, and lease terms indicated in those tables shall form binding contractual obligations.

3.2.1 Common Service Elements Applicable to All Selected Categories

For each category selected in the Procurement Summary Tables, the scope shall include the associated service elements required under the procurement documents, including, as applicable:

a) delivery and deployment;

b) configuration and commissioning;

c) service desk and technical support;

d) maintenance and break/fix;

e) replacement and refresh;

f) asset and configuration record-keeping;

g) monitoring and reporting;

h) acceptance, evidence, and service documentation; and

i) return, disposal, and transition support.

3.3 Assessment and Baseline Validation

Where requested by the Contracting Authority in connection with any selected service category, before commencement of deployment for the relevant in-scope category, the Contractor shall perform an assessment and baseline validation exercise sufficient to confirm the operational requirements, user profiles, service-class mapping, deployment assumptions, asset baseline, site-specific constraints, and implementation dependencies applicable to that category.

Such assessment or pre-assessment may include, as applicable:

a) identification and validation of user groups and their corresponding service-class requirements;

b) confirmation of indicative quantities, locations, and deployment priorities;

c) review of the existing asset baseline and replacement assumptions;

d) identification of compatibility, configuration, connectivity, support, security, and logistical dependencies;

e) validation of any prerequisites for installation, rollout, migration, onboarding, or service activation; and

f) preparation of recommendations, implementation assumptions, or a deployment and transition plan, where requested by the Contracting Authority.

Where the assessment identifies inconsistencies, omissions, incorrect user-to-class mapping, missing prerequisites, or other conditions that may materially affect successful implementation, the Contractor shall promptly notify the Contracting Authority and, where required, submit recommendations for corrective action before proceeding with the relevant activity.

Any assessment outputs shall form part of the Contractor's implementation documentation and shall be updated where approved changes to scope, users, locations, or service volumes make such update necessary.

3.4 Service Delivery and Accountability Model

The intended future model is a single integrated service contract with one Prime Contractor or Lead Member accountable for the full service delivery model. The Prime Contractor or Lead Member may rely on consortium members, subcontractors, OEM partners, distributors, leasing/financing partners, managed service partners or specialist suppliers, but such arrangements must not fragment accountability.

a) one accountable contractual counterparty or Lead Member for all service towers;

b) clear responsibility matrix for each participant in the delivery chain;

c) flow-down of all security, confidentiality, SLA, reporting, audit, acceptance, subcontractor and exit obligations;

d) single service-management and governance model across all towers;

e) single reporting framework and consolidated performance visibility;

f) single escalation route for contractual, operational and security matters;

g) clear interface management between OEMs, local partners, lessors, distributors and service providers.

4. Baseline Volumes and Service Class Framework

This Section establishes the baseline volume assumptions and the service-class framework to be used for proposal preparation, service profiling, deployment planning, pricing, ordering, support, refresh, and contract management.

The baseline volumes set out in this Section are intended to provide a common planning and pricing basis for the procurement. They shall not, by themselves, constitute the final binding quantities under the Contract, which shall be determined by the Procurement Summary Tables, the Price Schedule, approved deployment plans, and any lawful adjustments made in accordance with the Contract.

4.1 Baseline Volumes

For proposal preparation and initial implementation planning, the baseline end-user population shall be assumed to be approximately 1,200 to 1,300 users.

This baseline shall be used by Bidders for the purposes of:

a) preparing technical and commercial proposals;

b) structuring delivery capacity, support coverage, and operational arrangements;

c) estimating deployment waves, refresh planning, and replacement volumes;

d) preparing pricing for the initial service baseline and any approved optional scaling; and

e) demonstrating operational readiness for the pilot scope.

The baseline population represents an indicative planning assumption for the pilot. The actual quantities to be deployed under the Contract shall be those recorded in the Procurement Summary Tables and the approved deployment and activation records.

For the avoidance of doubt:

a) the baseline volume shall be treated as a procurement and pricing assumption for the pilot;

b) the final contractual quantities may be lower or higher than the baseline for particular classes, categories, or deployment phases, subject to the Procurement Summary Tables and the Contract; and

c) payment shall be governed by the pricing model and actual deployed and accepted service quantities in accordance with the Contract.

Baseline quantities for network equipment and any optional categories shall be determined through the Procurement Summary Tables and the applicable Conformity Tables.

4.2 Service Class Framework

The service-class framework shall be the primary mechanism for defining the approved end-user computing profiles under the Contract. Each class represents a distinct service profile intended to match user roles, mobility requirements, performance needs, and operational use cases.

The Contractor shall provide services in accordance with the following class framework:

Class	Service type	Target users	Indicative profile
1-2	Basic WaaS	Administrative staff	Standard laptop class; baseline productivity profile 8GB RAM
3-4	Mobile WaaS	Field workers, executives	Lightweight / touch capable profile where applicable
5-6	Performance WaaS	Analysts, engineers, heavy users	Higher-performance laptop profile 16–32GB RAM
7	Tablet service	Inspectors, highly mobile staff	Tablet / rugged tablet profile with mobility features
8-9	Chromebook service	Cloud-centric users	Chrome OS-based profile
10	DaaS	Specialized users	Desktop-as-a-service / cloud desktop profile
11	VDI	High-security or centrally managed users	Virtual desktop infrastructure profile

The service classes shall be used for the following purposes:

a) user profiling and service assignment;

b) technical specification and conformity assessment;

c) pricing and billing structure;

d) deployment and rollout planning;

e) support and refresh planning; and

f) reporting on service volumes and class distribution.

The indicative profiles set out above are intended to support consistent classification and proposal preparation. The detailed technical requirements for each class shall be governed by the applicable Conformity Tables and related annexes.

4.2.1 Configuration Response Rules

Bidders shall prepare their technical proposals in accordance with the approved service-class framework and the applicable Conformity Tables.

For the purposes of bid responsiveness and technical evaluation:

a) the Bidder shall respond to each configuration category expressly required by the procurement documents;

b) where a configuration category is requested, the Bidder shall respond to all mandatory configurations within that category;

c) the specifications set out in the applicable Conformity Tables shall be treated as minimum requirements unless expressly stated otherwise;

d) any proposed alternative shall be accepted only where the procurement documents permit equivalent or better solutions and where the Bidder clearly demonstrates full equivalence or superiority against each relevant requirement;

e) no Bidder may selectively omit a mandatory configuration, reduce a mandatory requirement, or structure a response in a manner that defeats comparability across bids; and

f) the Bidder shall complete the applicable compliance schedules and Conformity Tables in full, with clear references to the proposed make, model, service profile, and supporting evidence.

Technical annex rule: The conformity tables remain the controlling technical minimums for laptops, network devices, printers, VoIP, Wi-Fi, routers, firewalls, and related categories. This ToR defines the service and delivery obligations that sit around those technical annexes.

A proposal that does not respond to the required configuration categories, omits mandatory configurations, or fails to demonstrate compliance with the applicable minimum requirements may be treated as non-responsive to the extent provided in the procurement documents.

4.3 Class Allocation and Baseline Validation

The initial allocation of users to service classes shall be determined by the Contracting Authority on the basis of operational need, approved internal planning, and any assessment or baseline validation exercise carried out in accordance with Section 3.

Where requested by the Contracting Authority, the Contractor shall support the validation or refinement of class allocation by reviewing user profiles, roles, performance needs, mobility requirements, and other relevant operational criteria. Any such support shall be advisory in nature unless and until the Contracting Authority approves the resulting class allocation for contractual use.

Each end user shall be assigned to the service class that most closely corresponds to the approved functional and operational requirement. No class assignment shall be made solely for commercial convenience where such assignment would result in material over-specification, under-specification, or misalignment with actual need.

The approved service-class allocation shall form the basis for:

a) the initial deployment plan;

b) the class-based volume assumptions recorded in the Procurement Summary Tables;

c) the pricing and billing structure under the Contract;

d) the refresh and replacement cycle for the relevant users or device groups; and

e) the reporting of active service volumes by class.

4.4 Baseline Adjustment and Volume Flexibility

The baseline volumes and class allocations may be adjusted during the term of the Contract in accordance with:

a) approved deployment and activation records;

b) additions, removals, redeployments, or reclassifications of users;

c) approved changes in operational requirements or staffing structure;

d) refresh, replacement, or migration requirements; and

e) the change-control and commercial adjustment provisions of the Contract.

Any adjustment to baseline volumes or service-class allocations shall be documented in accordance with the Contract and shall not take effect for billing or service management purposes unless properly approved and recorded through the applicable contractual mechanism.

Where a user is reassigned from one service class to another, the applicable service, support, and pricing consequences shall apply from the effective date of the approved reclassification.

4.5 Relationship to Technical and Commercial Annexes

This Section shall be read together with:

a) the Procurement Summary Tables;

b) the applicable Conformity Tables;

c) the Price Schedule;

d) the Service Level requirements; and

e) the deployment, activation, and acceptance records maintained under the Contract.

In the event of any inconsistency between the indicative baseline assumptions in this Section and the binding quantities or allocations recorded in the contractual annexes and approved implementation records, the latter shall prevail.

5. Governance and Service Management Services

The Contractor shall establish, implement, and maintain a governance and service management model for all services delivered under the Contract. Such model shall ensure clear oversight, defined roles and responsibilities, documented service-management processes, regular performance review, effective escalation, controlled change management, and continuous service improvement throughout the contract term.

The governance and service management model shall operate at strategic, operational, and technical levels and shall support effective coordination between the Contracting Authority, the Contractor,

and any approved subcontractors or service partners involved in service delivery. The Contractor shall ensure that the model is sufficiently robust to support contract oversight, service performance monitoring, issue resolution, decision-making, and orderly management of risks, changes, and dependencies across the in-scope services.

5.1 Governance Framework

The Contractor shall maintain a governance framework that provides an effective means to:

a) oversee the delivery of the services;

b) review service performance, service levels, operational issues, and service risks on a regular basis;

c) resolve matters at the lowest effective governance level;

d) escalate matters requiring higher-level review or decision-making;

e) manage service changes, including technical, operational, commercial, and scope-related changes, through the agreed change-control process; and

f) support service improvement, service stabilization, and orderly contract management throughout the term of the Contract.

The governance framework shall include, at a minimum:

a) a **strategic governance level** for executive oversight and escalated decisions;

b) an **operational governance level** for routine contract and service management;

c) a **technical working level** for detailed technical coordination and issue resolution; and

d) a **change governance function**, including a Change Advisory Board or equivalent forum, for the review and processing of changes in accordance with the Contract.

5.2 Governance Roles and Responsibilities

The Contractor shall designate, maintain, and keep continuously available the governance and service management roles necessary for the proper performance of the services. At a minimum, these roles shall include:

a) a **Contract Manager**, responsible for overall contractual coordination, formal communications, issue escalation, and management of contractual obligations;

b) a **Service Manager**, responsible for day-to-day service governance, service quality, service-level management, and adherence to documented service-management processes;

c) a **Security Focal Point**, responsible for operational coordination of security-related matters, security issue escalation, security reporting, and coordination of response activities within the scope of the Contract;

d) a **Service Desk Manager** or equivalent operational lead, responsible for service desk performance, ticket governance, and operational reporting; and

e) such additional transition, technical, asset-management, reporting, or specialist roles as may be necessary for the selected services.

The Contracting Authority shall designate the corresponding representatives necessary for contract governance, including those responsible for contract management, operational coordination, security coordination, acceptance, and change approval.

The Contractor shall ensure that all designated roles are assigned to suitably qualified personnel with sufficient authority, competence, and availability to discharge their responsibilities effectively. Any replacement of key governance or service management personnel shall be subject to the notification and substitution requirements of the Contract.

5.3 Governance Meetings and Review Structure

The Contractor shall participate in a formal meeting and review structure for the management of the services. Unless otherwise agreed, this structure shall include the following minimum governance layers:

5.3.1 Strategic Governance Review

A strategic governance review shall be held quarterly. This forum shall review overall contract performance, major service issues escalated from lower governance levels, strategic risks, major contractual matters, and decisions requiring executive direction.

5.3.2 Operational Governance Review

An operational governance review shall be held on a regular basis to review service performance, incidents, open issues, service-level attainment, transition progress where relevant, reporting outputs, and invoice-related operational matters. During transition and stabilization, such meetings may be held weekly or more frequently where justified by implementation intensity; thereafter, they shall normally be held monthly unless otherwise agreed.

5.3.3 Technical and Working-Level Reviews

Technical or working-level reviews shall be held as needed to address technical issues, implementation dependencies, compatibility matters, configuration concerns, service-improvement actions, and detailed operational topics that do not require executive intervention.

5.3.4 Change Advisory Board

A Change Advisory Board or equivalent change-review forum shall be convened as required to review and recommend approval, rejection, prioritization, sequencing, or amendment of relevant changes in accordance with the Contract's change-management provisions.

5.4 Service Management Model

The Contractor shall deliver the services in accordance with a documented and auditable service-management model based on established IT Service Management practices and aligned, at minimum, with **ISO/IEC 20000-1** or an equivalent recognized service-management framework.

The service-management model shall include, as applicable to the selected services:

a) service desk management;

b) incident management;

c) request fulfilment;

d) problem management;

e) change management;

f) configuration and asset management;

g) monitoring and event management;

h) capacity and performance management;

i) patch and vulnerability management; and

j) service reporting and continuous improvement.

The Contractor shall maintain the procedures, tools, records, and governance controls necessary to operate these processes in an auditable manner and to demonstrate compliance with the Contract.

5.5 Reporting, Escalation, and Continuous Improvement

The Contractor shall maintain a documented escalation structure for contractual, operational, technical, and security matters. Escalation procedures shall define:

a) escalation levels;

b) responsible roles;

c) trigger conditions;

d) expected response times for escalation handling; and

e) the route for escalation from operational review to executive review where necessary.

The Contractor shall provide regular service-management reporting in the form and frequency specified in the Contract, including operational reports, service-level reports, issue logs, action trackers, and such dashboards or supporting evidence as are required for governance purposes. Monthly service reviews shall address, at a minimum, SLA/KPI performance, open issues, service credits or penalties where applicable, invoicing matters, asset lifecycle matters, and agreed improvement actions.

The Contractor shall operate a continuous improvement process under which recurring incidents, service-level failures, user feedback, audit findings, and operational trends are reviewed and translated into corrective and preventive actions. Root cause analysis shall be performed for critical or recurring issues, and service-improvement actions shall be tracked through closure.

6. Transition Services

The Contractor shall provide all transition services necessary to move the selected services into operational use in a controlled, secure, and orderly manner, with minimum disruption to business operations.

6.1 Bidder Transition Proposal

The Bidder shall submit, as part of its Proposal, a transition methodology sufficient to demonstrate its understanding of the transition requirements and its capacity to implement the selected services.

The Bidder's transition submission shall include, as applicable:

a) the proposed transition approach and sequencing;

b) indicative phases, milestones, and timelines;

c) proposed staffing and key transition roles;

d) key assumptions, dependencies, and risks;

e) stabilization arrangements; and

f) fallback or rollback measures for critical activities.

6.2 Transition Plan After Award

Following contract award, the Contractor shall submit a detailed Transition Plan for approval by the Contracting Authority within the period specified in the Contract.

The Transition Plan shall include, as applicable:

a) the transition schedule and implementation sequence;

b) deployment waves, milestones, and readiness activities;

c) resource and staffing arrangements;

d) communications and user-coordination activities;

e) transition deliverables and reporting arrangements;

f) escalation, fallback, and rollback measures; and

g) transition risks, dependencies, and mitigation measures.

No material transition activity shall commence until the Transition Plan has been approved by the Contracting Authority.

6.3 Deployment and Stabilization

The Contractor shall perform deployment and transition in accordance with the approved Transition Plan and in such phases or waves as are necessary to maintain continuity of operations.

Transition activities shall include, as applicable:

a) mobilization and readiness activities;

b) delivery, installation, onboarding, or service activation;

c) user support during rollout;

d) stabilization support following deployment; and

e) submission of the required transition records and implementation documentation.

Where pilot or phased rollout is used, progression to the next phase shall be subject to the approved transition approach and any acceptance or readiness requirements specified in the Contract.

6.4 Assumptions, Dependencies, and Completion

The Contractor shall identify and manage the assumptions and dependencies relevant to transition, including those relating to access, site readiness, user availability, approvals, technical prerequisites, and information required for implementation.

Where a dependency is not satisfied or a material issue arises that may affect the transition timeline, quality, or readiness of the services, the Contractor shall promptly notify the Contracting Authority and submit the proposed corrective action or revised implementation approach.

Transition for the relevant service, category, or phase shall be deemed complete only when:

a) the approved transition activities have been performed;

b) the required transition deliverables and records have been submitted;

c) the relevant services have entered stable operational use; and

d) completion has been confirmed in accordance with the Contract.

7. Service Desk Services

7.1 General requirements

The Contractor shall operate a centralized Service Desk as the single point of contact for incidents, service requests, user communications, and support coordination. The Service Desk shall support, at a minimum, telephone, portal, email, and any other channel approved by the Contracting Authority.

The Bidder shall submit, as part of its Proposal, a description of the proposed Service Desk model sufficient to demonstrate its capacity to support the selected services. The submission shall describe the proposed operating model, service coverage, support channels, service hours, ticketing and escalation approach, the interface with remote, desk-side, field, and specialist support, where relevant, the proposed knowledge-base and user-support approach, and the reporting outputs to be provided. The submission shall be sufficiently detailed to enable the Contracting Authority to assess the feasibility, responsiveness, and operational suitability of the proposed Service Desk model.

7.2 Service Desk scope

The Service Desk scope shall include, as applicable:

a) incident intake, triage, classification, prioritization, and routing;

b) service request intake and fulfilment coordination;

c) first-line troubleshooting and remote resolution;

d) major-incident communications and escalation management;

e) knowledge-base maintenance and user guidance;

f) ticket quality assurance and closure validation; and

g) service analytics, first-call resolution tracking, backlog control, and user satisfaction measurement.

7.3 Support hours and language

The minimum support window shall be aligned with the final SLA schedule. The Contractor shall clearly state standard hours, extended coverage options, on-call escalation model, and language

support available. Any deviations from mandatory coverage requirements shall be explicitly identified in the proposal.

7.4 Ticketing and records

All incidents and service requests shall be logged in the Contracting Authority-approved or Contractor-provided system, as agreed, with full auditability, timestamps, categorization, ownership, and evidence of actions taken. The Contractor shall maintain an up-to-date ticket taxonomy, severity matrix, and escalation tree.

8. Incident and Request Management

The Contractor shall establish and operate an incident and request management process for all selected services under the Contract. The process shall ensure that incidents and service requests are recorded, classified, prioritized, routed, resolved, fulfilled, and closed in a controlled, auditable, and timely manner.

8.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed incident and request management approach sufficient to demonstrate its capacity to support the selected services. The submission shall describe the proposed process for intake, categorization, prioritization, routing, escalation, fulfilment, closure, user communication, and coordination with service desk, desk-side, field, technical, and specialist support functions, where relevant.

The incident and request management approach shall be sufficiently detailed to enable the Contracting Authority to assess the feasibility, responsiveness, and operational suitability of the proposed operating model.

8.2 Incident management

The Contractor shall manage all incidents affecting the in-scope services through a documented process designed to restore normal service operation as quickly as reasonably possible and to minimize operational impact.

The incident management process shall include, as applicable:

a) incident logging and unique ticket identification;

b) categorization, prioritization, and severity assignment;

c) triage and initial diagnosis;

d) escalation to the appropriate support level where required;

e) resolution, service restoration, or work-around implementation;

f) user communication and status updates; and

g) closure with documented resolution details.

The Contractor shall ensure that critical or high-impact incidents are escalated without delay and managed in accordance with the applicable escalation path, communication requirements, and service levels set out in the Contract.

8.3 Service request management

The Contractor shall manage service requests through a documented request fulfilment process. The process shall apply to all in-scope requests that do not constitute incidents, including routine user requests, standard service actions, access-related requests where applicable, approved moves, additions, changes, equipment exchanges, and other defined support requests within the scope of the Contract.

The service request process shall include, as applicable:

a) request logging and categorization;

b) validation of request type and entitlement;

c) routing to the responsible fulfilment function;

d) coordination of approvals where required under the Contract or agreed procedures;

e) fulfilment and confirmation of completion; and

f) closure with appropriate supporting records.

8.4 Prioritization and escalation

The Contractor shall maintain and apply a documented prioritization and escalation framework for incidents and service requests. The framework shall include a severity matrix, escalation thresholds, ownership rules, and the route for escalation to higher support levels or management review where necessary.

The Bidder shall describe, in its Proposal, the proposed prioritization and escalation approach, including the treatment of major incidents, recurring incidents, aged tickets, stalled requests, and requests or incidents requiring coordination across multiple support functions.

8.5 Major incidents

The Contractor shall maintain a defined process for the handling of major incidents affecting critical users, critical services, or multiple users. Such process shall include immediate escalation, coordinated response management, regular status communication, business-facing updates where required, and post-incident review.

Where a major incident occurs, the Contractor shall ensure that the incident is actively managed until service is restored or an agreed work-around is in place, and that the relevant records, communications, actions taken, and resolution status are fully documented.

8.6 Closure, records, and reporting

The Contractor shall ensure that incidents and service requests are not closed until the relevant action has been completed, the resolution or fulfilment has been properly recorded, and the ticket record contains sufficient evidence of the steps taken.

The Contractor shall maintain accurate and auditable records of incidents and service requests, including classification, timestamps, ownership, escalations, actions performed, status history, and closure details. The Contractor shall provide reporting on incident and request management in the form and frequency specified in the Contract. Such reporting shall include, as applicable:

a) ticket volumes by type, category, and severity;

b) response and resolution performance;

c) request fulfilment performance;

d) backlog and ageing analysis;

e) major incident statistics;

f) recurring incident and repeat-request trends; and

g) escalation volumes and unresolved ticket analysis.

9. Field and Desk-Side Support Services

The Contractor shall provide field and desk-side support services for the selected categories of equipment and services under the Contract where remote support, centralized handling, or standard request fulfilment is not sufficient to resolve the issue or complete the required activity.

9.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed field and desk-side support model sufficient to demonstrate its capacity to support the selected services. The submission shall describe the proposed operating model, service coverage, dispatch approach, site attendance arrangements, interface with the Service Desk and other support functions, and the means by which on-site activities will be controlled, recorded, and completed.

The field and desk-side support approach shall be sufficiently detailed to enable the Contracting Authority to assess the feasibility, responsiveness, and operational suitability of the proposed support model.

9.2 Scope of field and desk-side support

The Contractor shall provide field and desk-side support services for incidents, service requests, installations, replacements, exchanges, relocations, and other support actions requiring physical intervention at the relevant site or user location.

The scope of such support shall include, as applicable:
a) on-site troubleshooting and fault resolution;
b) desk-side user support where remote resolution is not sufficient;
c) equipment installation, swap-out, replacement, and collection;
d) support for moves, adds, and changes within the approved scope;
e) coordination of parts, spares, loan devices, or replacement units where required; and
f) confirmation of completion and update of the relevant service and asset records.

9.3 Dispatch and site attendance

The Contractor shall maintain a documented process for the dispatch and control of field and desk-side support activities. This process shall ensure that on-site support is initiated, tracked, escalated, and completed in accordance with the applicable service levels and operational procedures.

The Bidder shall describe, in its Proposal, the proposed dispatch model, territorial or location coverage, attendance arrangements, escalation path, and any assumptions relevant to site access, scheduling, or logistical support.

Where site attendance is required, the Contractor shall ensure that the relevant support personnel attend with the tools, parts, equipment, information, and authorizations reasonably necessary to perform the required activity efficiently and safely.

9.4 Coordination with other support functions

Field and desk-side support shall operate as part of the overall service management model and shall be coordinated with the Service Desk, incident and request management processes, asset and configuration records, and any relevant technical or specialist support functions.

The Contractor shall ensure that hand-offs between remote support, field support, specialist support, and third-party support are clearly controlled and recorded, and that ownership of the activity remains visible at all times.

9.5 Records, completion, and reporting

The Contractor shall ensure that all field and desk-side support activities are properly recorded in the relevant service-management system or agreed operational records. Such records shall include, as applicable, the reason for dispatch, the activity performed, equipment handled, replacement or collection details, user confirmation where appropriate, and the final status of the activity.

The Contractor shall provide reporting on field and desk-side support in the form and frequency specified in the Contract. Such reporting shall include, as applicable, dispatch volumes, attendance performance, resolution outcomes, repeat visits, replacement activity, and any material issues affecting service quality or continuity.

10. Configuration and Asset Management

The Contractor shall establish and maintain configuration and asset management arrangements for all selected services under the Contract. Such arrangements shall ensure accurate identification, recording, tracking, reconciliation, and lifecycle control of in-scope equipment, related configurations, and associated service records.

10.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed configuration and asset management approach sufficient to demonstrate its capacity to control the selected services throughout their lifecycle. The submission shall describe the proposed asset register or CMDB approach, record structure, update process, reconciliation method, ownership and location tracking, handling of refresh and replacement events, and the reporting outputs to be provided.

The Contractor shall maintain a complete and up-to-date configuration and asset record for all in-scope equipment and service units under its responsibility. The configuration and asset management approach shall support planning, deployment, operation, refresh, return, disposal, and auditability throughout the contract term.

10.2 Configuration and asset records

The Contractor shall maintain records sufficient to identify each in-scope asset or service unit and to track its status throughout the lifecycle. Such records shall include, as applicable, asset type, class, make and model, serial number, asset tag, assigned user, location, deployment status, configuration baseline, warranty or support status, lease status, refresh status, return status, and any other information required under the Contract.

Where agreed under the Contract, the Contractor shall maintain or interface with a CMDB, asset inventory, or equivalent control register and shall ensure that updates arising from deployment, moves, adds, changes, replacements, refresh, return, or disposal are recorded in a timely and auditable manner.

10.3 Lifecycle control and reconciliation

The Contractor shall operate a configuration and asset management process capable of supporting the lifecycle control of all selected categories of equipment and services. This shall include, as applicable, initial registration, deployment tracking, user assignment, location tracking, configuration updates, replacement and refresh tracking, returns processing, and end-of-service handling.

The Contractor shall perform periodic reconciliation of the relevant asset and configuration records against the deployed environment, the approved deployment records, and any other agreed control sources. Where discrepancies, missing records, incorrect assignments, data variances, or unaccounted-for assets are identified, the Contractor shall investigate, correct, and document the outcome without undue delay.

10.4 Reporting, evidence, and audit support

The Contractor shall provide configuration and asset management reporting in the form and frequency specified in the Contract. Such reporting shall include, as applicable, asset inventory status, class distribution, location and assignment status, refresh status, non-deployed or returned assets, data-quality or reconciliation exceptions, and any evidence required to support invoicing, acceptance, returns, secure wipe, disposal, or audit requests.

The Contractor shall maintain records and evidence sufficient to support verification of actual deployed assets and service units, asset lifecycle events, and compliance with the Contract. Where requested, the Contractor shall provide supporting records for audit, review, reconciliation, acceptance, or contract-management purposes.

11. Monitoring, Reporting, and Service Levels

The Contractor shall establish and maintain monitoring, reporting, and service-level management arrangements for all selected services under the Contract. Such arrangements shall ensure that service performance is measurable, auditable, and capable of ongoing review against the requirements of the Contract.

11.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed monitoring, reporting, and service-level management approach sufficient to demonstrate its capacity to manage and evidence service performance. The submission shall describe the proposed monitoring model, reporting outputs, measurement method, service-level governance approach, and the means by which performance data will be collected, validated, and presented.

The Contractor shall maintain monitoring and reporting capabilities sufficient to support operational control, service review, performance management, escalation, and verification of compliance with the Contract.

11.2 Monitoring requirements

The Contractor shall monitor the performance and status of the selected services, service components, and related support activities to the extent necessary to manage service delivery and demonstrate compliance with the Contract.

Monitoring shall include, as applicable, service availability, ticket status, response and resolution performance, deployment status, asset status, replacement and refresh activity, and any other performance indicators required under the Contract. Where automated monitoring is used, the Contractor shall ensure that the relevant data is retained, traceable, and capable of supporting reporting and audit.

Where the monitoring arrangements identify an actual or impending service failure, breach of service level, recurring issue, or material degradation in service quality, the Contractor shall take prompt corrective action and record the relevant outcome.

11.3 Reporting requirements

The Contractor shall provide regular service reporting in the form and frequency specified in the Contract. The Bidder shall describe, in its Proposal, the proposed reporting approach, including the format, frequency, and content of the reports to be provided.

Service reporting shall include, as applicable, service performance against service levels and KPIs, incident and request volumes, backlog and ageing analysis, major service issues, escalation volumes, deployment and transition status where relevant, asset and refresh status, and any other information reasonably required for contract management and service oversight.

Reports shall be sufficiently clear, complete, and timely to enable the Contracting Authority to assess service performance, identify trends, review exceptions, and take informed management decisions.

11.4 Service levels and KPI requirements

The services shall be governed by the service levels and KPIs set out in the SLA Schedule and related annexes to the Contract. The Bidder shall confirm its ability to meet the applicable service levels and shall clearly identify any proposed assumptions, dependencies, exclusions, or deviations affecting service-level performance.

The Contractor shall measure and report service-level performance in accordance with the Contract and shall maintain the records and evidence necessary to substantiate the results reported. Where service-level failures, repeated KPI breaches, or material negative trends are identified, the Contractor shall investigate the cause, propose corrective measures, and implement the agreed actions in accordance with the Contract.

Service-level measurement, reporting, and review shall support the application of service credits, performance remedies, escalation measures, or other contractual consequences where such measures are provided for under the Contract.

The KPI set below is indicative and shall be read together with, and subject to, the final SLA Schedule and related annexes.

KPI	Target basis	Measurement
Service availability	As per SLA schedule	Automated monitoring / service evidence
Critical incident response	As per SLA schedule	Ticket timestamps
Critical incident resolution	As per SLA schedule	Closure evidence
Standard incident response and resolution	As per SLA schedule	Ticket metrics
First-call resolution	Tracked monthly	Service desk analytics
User satisfaction	Tracked monthly / quarterly	Survey results
Patch compliance	Tracked monthly	Compliance dashboards
Asset accuracy	Tracked monthly	Inventory reconciliation

12. Managed Network, Print, and VoIP / Conference Services

12.1 Network services

Where included in the final order schedule, the Contractor shall supply, install, configure, monitor, maintain, and support switches, routers, Wi-Fi access points, and firewalls / SD-WAN equipment in accordance with the applicable conformity tables and approved architecture.

12.2 Print services

Where included in the final order schedule, the Contractor shall provide managed print services including fleet deployment, consumables workflow where applicable, maintenance, repairs, secure print functionality where required, meter collection, and reporting.

12.3 VoIP and conference equipment services

Where included in the final order schedule, the Contractor shall provide managed IP telephony and conference equipment services, including support, maintenance, replacement coordination, event logging, and integration with the Contracting Authority's approved communication environment.

13. Security Operations, Patch Management, and Vulnerability Management

The Contractor shall establish and maintain security operations, patch management, and vulnerability management arrangements for all selected services under the Contract. Such arrangements shall ensure that in-scope equipment, configurations, and service components are operated in a secure manner, that security weaknesses are identified and addressed in a timely manner, and that security-related activities are documented, traceable, and auditable.

13.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed security operations, patch management, and vulnerability management approach sufficient to demonstrate its capacity to protect the selected services throughout their lifecycle. The submission shall describe the proposed operating model, governance approach, roles and responsibilities, patching and remediation process, vulnerability handling process, exception handling, and the reporting outputs to be provided.

The Contractor shall maintain security procedures, tools, records, and controls sufficient to support secure operation of the selected services and to demonstrate compliance with the Contract and the Security Schedule.

13.2 Security operations requirements

The Contractor shall perform the operational security activities necessary for the selected services, including the application of approved security baselines, maintenance of secure configurations, review of security events within the scope of the Contract, escalation of security-related issues, and coordination of response actions with the Contracting Authority and other relevant support functions.

Where a security event, suspected compromise, policy breach, or material weakness affecting the selected services is identified, the Contractor shall record the matter, take the immediate containment or corrective actions required within its scope, and notify the Contracting Authority in accordance with the Contract and the applicable incident and escalation procedures.

13.3 Patch management requirements

The Contractor shall operate a documented patch management process for all in-scope components for which patching is within the scope of the Contract. The process shall cover patch identification, testing or validation where required, scheduling, deployment, exception handling, rollback where necessary, and evidence of completion.

The Bidder shall describe, in its Proposal, the proposed patch management methodology, patching cadence, prioritization logic, emergency patch process, maintenance-window assumptions, and the means by which patch compliance will be measured and reported.

The Contractor shall ensure that security patches, critical patches, and other required updates are applied within the timelines specified in the Contract or the Security Schedule. Where a patch cannot be applied within the required timeframe, the Contractor shall document the reason, assess the associated risk, implement any required interim control or mitigation, and obtain the necessary approval for deferment where such approval is required.

13.4 Vulnerability management requirements

The Contractor shall operate a documented vulnerability management process for all in-scope components for which vulnerability management is within the scope of the Contract. The process shall include vulnerability identification, assessment, classification, remediation planning, remediation tracking, revalidation where required, and closure.

The Bidder shall describe, in its Proposal, the proposed vulnerability management methodology, severity assessment approach, remediation workflow, treatment of recurring vulnerabilities, exception handling, and reporting approach.

Where vulnerabilities are identified, the Contractor shall assess their relevance to the selected services, determine the required remediation or mitigation action, and address them within the timelines specified in the Contract or the Security Schedule. Where remediation is not immediately possible, the Contractor shall document the reason, record the risk, implement interim mitigation where required, and track the matter through resolution or approved exception.

13.5 Records, evidence, and reporting

The Contractor shall maintain records sufficient to demonstrate the performance of security operations, patch management, and vulnerability management activities. Such records shall include, as applicable, patch status, exception records, vulnerability status, remediation actions, security-related escalations, risk acceptances, and evidence of closure or mitigation.

The Contractor shall provide reporting in the form and frequency specified in the Contract. Such reporting shall include, as applicable, patch compliance status, overdue patches, vulnerability status by severity, outstanding remediation items, approved exceptions, recurring issues, and any material security-related trends affecting the selected services.

Where required by the Contract, the Contractor shall support audit, review, and verification activities relating to security operations, patch management, and vulnerability management and shall provide the relevant supporting evidence upon request.

14. Acceptance, Evidence, and Documentation

The Contractor shall provide all evidence, records, and documentation necessary to enable the Contracting Authority to verify that the selected services, equipment, and related deliverables have been provided in accordance with the Contract. Acceptance shall be based on the applicable contractual requirements, including the Technical Specifications, Conformity Tables, Procurement Summary Tables, Service Level requirements, Security Schedule, approved deployment or transition records, and any other acceptance criteria expressly stated in the Contract.

14.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed acceptance and evidence approach sufficient to demonstrate its capacity to support verification, approval, and audit of the selected services. The submission shall describe the proposed acceptance process, the evidence to be provided, the supporting documentation to be maintained, and the means by which non-conformities, defects, or outstanding items will be recorded and resolved.

The Contractor shall maintain an acceptance and documentation process sufficient to support orderly delivery verification, service activation, record completeness, and contract administration throughout the contract term.

14.2 Acceptance requirements

The Contractor shall ensure that no service, equipment item, deployment activity, replacement, refresh, return, or other deliverable is presented for acceptance unless the relevant activity has been completed in accordance with the Contract and the required evidence is available.

Acceptance may apply, as relevant to the Contract, to individual items, batches, deployment waves, service activations, replacements, refresh events, configuration changes, returns, or other defined deliverables. The applicable acceptance method, evidence set, and approval route shall be those specified in the Contract.

Where the Contracting Authority identifies a defect, non-conformity, missing record, incomplete activity, or other deficiency affecting acceptance, the Contractor shall correct the matter and resubmit the relevant deliverable or evidence for review within the period specified in the Contract or otherwise agreed.

Acceptance evidence:

- technical compliance against the applicable conformity tables;
- serial number and delivery records;
- installation / deployment checklists;
- configuration and hardening evidence;

- testing records and pass/fail results;
- asset registration evidence;
- training / knowledge transfer evidence where applicable;
- security baseline confirmation and incident / escalation readiness evidence.

Milestone acceptance:

The Contracting Authority may use interim acceptance, partial acceptance, pilot acceptance, and final acceptance depending on the deployment structure. Rejected or conditionally accepted deliverables shall be remediated by the Contractor at no additional cost and resubmitted for validation.

14.3 Evidence and supporting records

The Contractor shall provide the evidence required to support acceptance, verification, and audit of the services and deliverables. Such evidence shall include, as applicable, delivery records, serial numbers, asset tags, installation records, configuration records, test results, deployment confirmations, user assignment records, acceptance forms, secure wipe certificates, disposal records, training completion records, and any other documentation required under the Contract.

All evidence shall be accurate, traceable, and capable of being linked to the relevant item, activity, service unit, deployment event, or service record. Where evidence is maintained in electronic form, the Contractor shall ensure that it is accessible, complete, and capable of being produced upon request.

14.4 Documentation requirements

The Contractor shall prepare, maintain, and keep current the documentation necessary for the proper performance, control, and verification of the selected services. Such documentation shall include, as applicable, technical documentation, operational procedures, user guidance, configuration records, asset records, transition records, support records, reporting outputs, security-related records within scope, and any other documents required by the Contract.

Where the Contract requires the submission, approval, or update of specific documents, the Contractor shall provide such documents in the required form and within the required timeframe. Superseded documents shall be retained or archived in accordance with the Contract and the applicable record-control requirements.

14.5 Conditional acceptance and outstanding items

Where the Contracting Authority grants conditional acceptance subject to minor deficiencies or outstanding items, the Contractor shall record such items, assign responsibility, and resolve them within the period specified in the Contract or otherwise agreed.

Conditional acceptance shall not relieve the Contractor of responsibility for full compliance with the Contract, nor shall it prevent the Contracting Authority from withholding final acceptance, payment, or other approvals where the relevant contractual conditions have not been satisfied.

14.6 Reporting and audit support

The Contractor shall maintain records sufficient to support acceptance status tracking, document completeness, and evidence review throughout the contract term. The Contractor shall provide, upon request, the documentation and supporting records necessary for review, reconciliation, audit, inspection, or contract management.

Where required by the Contract, the Contractor shall provide periodic reporting on acceptance status, outstanding acceptance items, rejected or resubmitted deliverables, missing evidence, and documentation completeness.

15. Exit, Return, Reversibility, and End-of-Service Obligations

The Contractor shall ensure that, upon expiry, termination, partial termination, replacement, refresh, or other end-of-service event, the selected services can be exited, returned, transferred, or otherwise concluded in a controlled, secure, and orderly manner, without avoidable disruption to operations and without loss of necessary data, records, or service continuity.

15.1 General requirements

The Bidder shall submit, as part of its Proposal, a description of the proposed exit and reversibility approach sufficient to demonstrate its capacity to support contract expiry, transition to a successor provider, return of in-scope equipment, secure wipe or disposal, knowledge transfer, and end-of-service handover.

The Contractor shall remain fully responsible for all exit and end-of-service obligations relating to the selected services, including those performed by subcontractors, consortium members, lessors, service partners, or other delivery partners.

15.2 Exit and transition-out requirements

The Contractor shall provide all transition-out services necessary to support an orderly exit from the Contract or from any selected service category. Such services shall include, as applicable, exit planning, service continuity support, knowledge transfer, handover of documentation and records, technical assistance, and coordination with the Contracting Authority and any successor provider.

The Contractor shall cooperate fully during the exit period and shall not take any action that would hinder transition, delay handover, or create avoidable dependency on the Contractor. Where required under the Contract, the Contractor shall continue to provide reasonable transition support for the period specified in the Contract.

15.3 Return, disposal, and secure erasure

Where in-scope equipment is to be returned, replaced, redeployed, disposed of, or otherwise removed from service, the Contractor shall perform the required decommissioning, preparation, packing, transport coordination, and record updates in accordance with the Contract.

Before any returned, redeployed, replaced, or disposed-of device leaves operational use, the Contractor shall perform secure data erasure in accordance with the Contract and the applicable security requirements. The Contractor shall provide certificates of secure wipe or equivalent evidence where required and shall ensure that no residual data remains accessible on decommissioned or reassigned equipment.

Where disposal or recycling is required, the Contractor shall ensure that it is carried out in accordance with the Contract and the applicable legal, environmental, and security requirements. Where lease return applies, the Contractor shall prepare and return the equipment in accordance with the applicable lease-return obligations.

15.4 Handover, records, and completion

The Contractor shall provide all documentation, records, configuration information, asset information, and other handover materials necessary to support continuity of service, auditability, and orderly transition at end of service.

Where required, the Contractor shall provide exportable records and data in a usable format, together with sufficient supporting information to enable continued use, transfer, reconciliation, or re-establishment of the relevant service components.

Exit or end-of-service obligations shall not be deemed complete until the required return, handover, secure wipe, documentation, and transition support activities have been performed and the relevant completion or acceptance requirements of the Contract have been satisfied.

16. Pricing and Commercial Response Requirements

16.1 Pricing structure

Bidders shall price the services using the official price schedules and shall clearly separate fixed recurring charges, one-time transition charges, optional expansion prices, and any variable or consumption-linked items allowed by the RFP.

Service tower	Pricing feedback requested
WaaS	Per user, per device, per class, per bundle or hybrid monthly fee; transition and refresh costs identified separately.
DaaS / VDI	Per named user, concurrent user, virtual desktop profile, platform component or hybrid model; assumptions on compute/platform dependencies clearly stated.
PraaS / Print as a Service	Per device monthly fee, cost-per-page, consumables-inclusive model, service bundle or hybrid structure.

NaaS	Per device, per port, per site, per security function, per managed network component or hybrid service fee.
UCaaS	Per handset, per extension, per user, per SIP channel/service component, per device bundle or hybrid model.
WLANaaS / WiFi as a Service	Per AP, per site, per managed WLAN component, per coverage area or hybrid model.
Meeting Room / Collaboration Equipment	Per room, per equipment set, per device, per support level or hybrid model.

16.2 Optional expansion pricing

The proposal shall include binding priced options for expansion of users, devices, service classes, sites, and associated service volumes within the contract term. Expansion pricing shall be scalable, transparent, and applicable without requiring a new tender, subject to Armenian law and formal Contracting Authority approvals.

16.3 Pricing discipline

- no hidden fees, undeclared mandatory licenses, or unexplained pass-through charges;
- clear unit-price logic by service class, user profile, and service tower;
- fixed recurring service charges;
- one-time transition, assessment, deployment or commissioning charges;
- priced expansion options for additional users, devices, sites, classes or service towers;
- variable or consumption-linked items and the controls needed to avoid hidden costs;
- spare pool, replacement, refresh, field support and site visit assumptions;
- indexation, foreign-exchange, financing, leasing, tax and customs assumptions where relevant;
- invoice evidence and automatic deduction/service credit logic.
- clear assumptions for spare pools, replacement cycles, site visits, and support coverage;
- invoice deductions / service credits to operate automatically where the contract so provides.

17. Bidder Response Instructions for the Technical Proposal

The Bidder shall submit a complete technical proposal demonstrating how the proposed solution satisfies the requirements of this Terms of Reference and the related procurement documents.

The technical proposal shall, at a minimum, include the following:

1) A detailed narrative response to each relevant section and sub-section of this Terms of Reference, clearly explaining how the Bidder proposes to meet the stated requirements.

2) A completed compliance matrix indicating, for each applicable requirement, whether the Bidder **Complies**, **Partially Complies**, or **Does Not Comply**. Any response other than full compliance shall be accompanied by a clear explanation, including the nature of the deviation, its operational impact, and any proposed alternative approach.

3) A description of the proposed service delivery model, including the respective roles and responsibilities of the Prime Contractor, the Lead Member, any consortium members, subcontractors, local partners, and other delivery participants, where applicable.

4) A description of the proposed mobilization approach, governance model, transition approach, Service Desk model, field and desk-side support model, security operations approach, and exit and reversibility approach, to the extent relevant to the selected services.

5) Evidence of relevant experience in public-sector environments or other comparably complex, multi-site, security-sensitive, or service-intensive environments, sufficient to demonstrate the Bidder's capacity to perform the Contract.

6) A dedicated schedule of assumptions, dependencies, exclusions, and bidder-requested clarifications. Such schedule shall be specific, necessary, and clearly presented, and shall not be used to qualify, reduce, or condition compliance with mandatory requirements of the procurement documents.

The Bidder shall ensure that the technical proposal is clear, internally consistent, and sufficiently detailed to enable the Contracting Authority to assess compliance, technical merit, operational suitability, implementation readiness, and overall responsiveness.

18. Final drafting rules for interpretation

- The words 'shall' and 'must' denote mandatory requirements.
- The word 'should' denotes a strong preference which may be departed from only where expressly justified and accepted by the Contracting Authority.
- In the event of ambiguity, the interpretation that better protects security, service continuity, data protection, and the Contracting Authority's operational interest shall prevail, subject to applicable law.
- Where this ToR and a technical annex both address the same subject matter, the more demanding requirement shall apply unless the RFP expressly states an order of precedence.