Terms of Reference

Table of Contents

1 Background and Overview of Requirements

1.1 Background

The European Stability Mechanism (the "**ESM**") is a permanent crisis resolution mechanism established by the euro area Member States as an intergovernmental organisation under public international law, with its seat and principal office at 6a, Circuit de la Foire Internationale, L-1347 Luxembourg (the "**ESM Building**" or the "**ESM Premises**"). Its purpose is to ensure the financial stability of the euro area as a whole and of its Member States experiencing severe financing problems by providing financial assistance through a number of instruments.

The ESM currently rents the underground, ground, first and second floors of the ESM Building, and some storage and archive areas on the first and second underground floors. The total rented area is approximately 9,374 m2 and provides about 300 workspaces, about 20 meeting rooms (capacity of 2-30 persons), a conference area (capacity of 200 persons on the first underground floor), and some other functional areas and rooms, e.g., server / technical, sanitary, small storages, UPS etc., located throughout the ESM Building.

The ESM also has access to two (2) other small ESM Sites.

The ESM requires the services of a single provider (the "**Provider**") to provide onsite IT support and other related services (the "**Services**") as described in these terms of reference (the "**Terms of Reference**" or "**ToR**").

The role of the Provider is not to only maintain business continuity of the Services, but also to add value in standardising and improving the quality of the Services, e.g., to be proactive in identifying improvements and delivering efficiencies.

Defined terms used throughout this Terms of Reference are set out in Annex 1 to this Terms of Reference "*TOR Annex 1 Definitions*".

1.2 Overview of Services

The ESM will award a framework agreement to a single Provider for the provision of the Services (the "**Framework Agreement**") for a period of four (4) years with an optional right to extend the term by two (2) years at the ESM's sole discretion.

The Provider will deliver the Services to ESM's End Users, currently around 380 users and 750 guest accounts, as well as users without an account, e.g., on-premise guests. The Services are to be performed at the ESM Premises unless otherwise indicated in the TOR.

The Provider will be required to cater to the high standards of the ESM user base, operate the Services with due care and to the highest security standards.

In the provision of the Services, the Provider will have to comply with SLRs and reporting requirements as described further below.

The ESM is heavily audited, so the Provider must have robust processes in place and pay great attention to detail in the execution of the Services. The Provider must keep all documentation related to the provision of the Services up to date at all times.

Note: At present, there are 10 full-time equivalent employees involved in the provision of the current service desk. The scope of the current service desk is, however, different to the scope set out herein. This detail is provided for information only and is not indicative of any specific ESM requirement or need.

For information only, the following annexes attached to these Terms of Reference also contain information on numbers of Incidents and Service Requests processed over specific periods of time for

the ESM. These numbers are not indicative of potential numbers going forward. The information in these annexes is for information only.

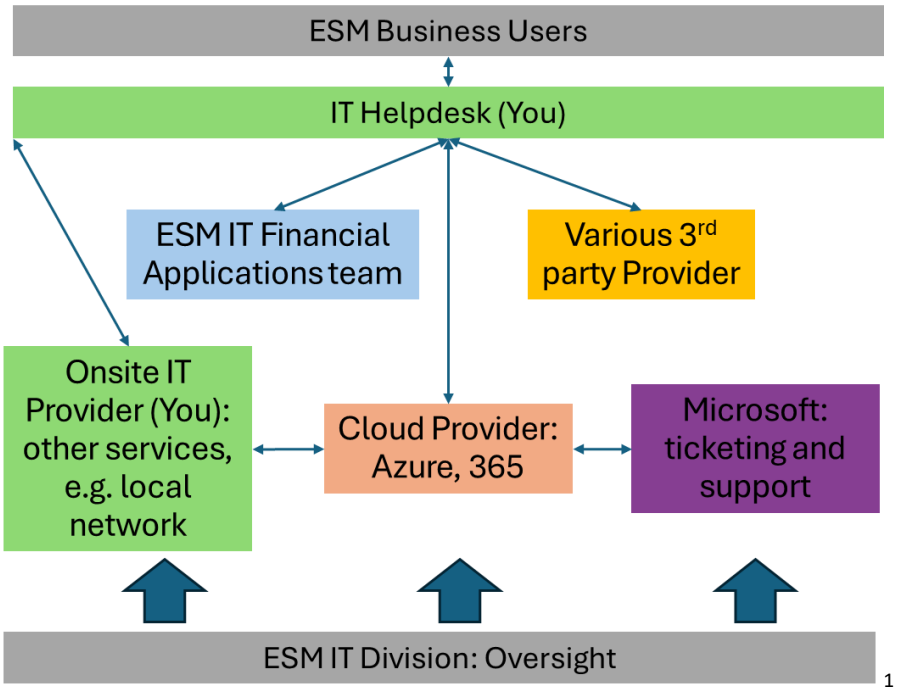
- TOR Annex 2 Amount of Incidents January 2020 to July 2024
- TOR Annex 3 Amount of Requests January 2020 to July 2024
- TOR Annex 4 Request Distribution Type January 2023 to December 2023 – This annex shows the different types of Service Requests raised by users within the period indicated.

1.3 Operational Information

The ESM Premises is open from 6 am to 10 pm on Business Days. These extended hours are provided to facilitate building maintenance and accommodate different working schedules. The Services will be provided by the Service Provider on a 24/7 basis except as set forth in these Terms of Reference.

The ESM IT Division is divided into functional teams responsible for, respectively, IT Corporate Systems, IT Financial Applications and IT Security. In order to ensure the proper execution of the Services, the Provider will be required to interact and cooperate with End Users, the ESM IT Division and the functional teams therein and various Third Party providers of the ESM, including but not limited to ESM's outsourced cloud platform management services provider.

The high-level graph of the environment in which the Provider will be required to operate in is presented below.



[1]

2 General service principles and service delivery management

2.1 General Service Principles

Throughout the term of the Framework Agreement, the Provider must adhere to the following general principles:

[1] "You" in this graph means the Provider.

(i) The Provider will have in place an IT Services model based on Best Industry Practice and accepted standards. All processes and defined terms referenced herein follow ITIL4 unless otherwise indicated. The Provider will adopt ITIL4 terminology and ITIL4-based practices to deliver the Services, ensuring smooth communication and service delivery through the integration with the ITIL-based terminology, tools, processes and procedures of the ESM.

(ii) The ESM process definitions precede Provider's process definitions.

(iii) The Provider will use ESM's system 'ServiceNow' as the primary ITSM Tool (the "**ESM ITSM Tool**") and the basis for the processes described, unless agreed otherwise. The Provider can alternatively choose to use its own ticketing system, but the ESM requires that Provider's tool connects to the ESM ITSM Tool at Provider's expense. The Provider may use its own specific tools for specific areas, e.g., within the delivery of a specific Service.

(iv) The ESM owns the authoritative Configuration Management Database/CMDB in the ESM ITSM Tool.

(v) The Provider will keep the required documentation, such as procedures and manuals, up-to-date and in line with the current working practices.

(vi) The Provider will maintain within the ESM ITSM Tool a knowledge base of known Problems, resolutions and other recurring Incidents in line with Best Industry Practice.

(vii) The Provider will ensure it keeps a robust audit trail for documentation of activities. The ESM's SharePoint and ESM ITSM Tool are considered the only safe locations to store and document information.

(viii) The Provider will comply with ESM Policies, ESM Procedures, standards and regulatory requirements applicable to the ESM for information, information systems, personnel, physical and technical security.

Note: ESM Policies and ESM Procedures, or parts thereof, relevant for the provision of the Services and the execution of the Framework Agreement, will be disclosed at Stage 2 of the procurement procedure Ref. No. IT/06/OS/MC/24.

(ix) The Provider will develop and maintain a comprehensive operation standards manual that contains standards, processes and procedures that will be used in the delivery of the Services in scope of this ToR. The manual will include clearly delineated roles and responsibilities, touchpoints and measurements between the ESM and the Provider. The manual will be shared with the ESM or other Third Parties upon request.

(x) The Provider must conform to changes in laws, regulations, compliance with internal and external audits, ESM Policies and ESM Procedures.

(xi) The ESM's working language is English. All documentation and communication are in English.

2.2 Service Integration

Service Integration refers to the service management processes that work across and within the various Services subject to this ToR.

Service Integration ensures that End-to-End Services are delivered seamlessly to End Users across interfaces and boundaries between providers delivering different parts of the End-to-End Service. The Provider is responsible for delivering Service Integration in conjunction with any Services the Provider provides under the Framework Agreement.

The Fees for the provision of the Services include any compensation due to the Provider for the provision of Service Integration activities. The Provider will not receive any separate compensation for the provision of the Service Integration activities.

Service Integration described in this Section 2.2 covers all production, test and development environments, and any other infrastructure environment as set out in this ToR.

Although this Section 2.2 is intended to describe the Service Integration comprehensively, the Provider shall be aware that this Section 2.2 is not all-inclusive in describing particular activities, resources or other details necessary for the Provider to perform the Service Integration properly.

Different categories of the Service Integration are described further below in this Section 2.2.

2.2.1 Change Management

The Provider will provide change management Services (**"Change Management Services"**) to ensure that Changes to the Services are managed according to ITIL principles and recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented, and reviewed in a controlled manner by the Provider. The Provider will ensure that all Changes are handled promptly and efficiently, recorded in the ESM ITSM Tool and where appropriate in the CMDB, and that overall business risk is reduced. A "**Change(s)**" means the addition, modification or removal of an authorised, planned or supported Service(s) or Service component(s) and its associated documentation.

The Provider will prepare and present all proposed Changes to the ESM for review. The ESM may accept, reject, or request further adaptations to the proposed Changes at its sole discretion. The Provider will accommodate all adaptations reasonably requested by the ESM. Once a Change is approved by the ESM, the Provider will execute the Change informing all impacted End Users of such Change. Where Changes impact IT infrastructure, the Provider will coordinate with all impacted stakeholders. Any Changes requiring an adjustment to the contractual arrangements between the Parties, will be agreed in writing.

2.2.2 Incident Management

The Provider will be responsible for Incident Management for the ESM and will manage Incidents as described in this section and in accordance with the applicable SLRs (the "**Incident Management Services**"). Failure of a Configuration Item that has not yet impacted a Service is also an Incident. The Provider will use Incident Management Services to return the Service to the End Users as quickly as possible and to minimise the adverse impact on the ESM's business operations.

The Provider will use Incident Management Services to return the Service to the End Users as quickly as possible and to minimise the adverse impact on the ESM's business operations. The Provider will detect Incidents on its own, as part of its ongoing performance of the Services and execution of the Framework Agreement, or by the End Users contacting the Service Desk or information and data facilitated to the Provider by the ESM IT Division or Third Parties.

Priority Levels

Incidents will be prioritised by priority levels ("**Priority Levels**"). Priority Levels are defined categories that identify the impact of the Incident and its urgency.

There are four Priority Levels:

(i) Priority Level 1 (P1);
(ii) Priority Level 2 (P2);
(iii) Priority Level 3 (P3); and
(iv) Priority Level 4 (P4),

as per the following description:

			IMPACT		
			High	Medium	Low
			Entire ESM or multiple departments affected	Multiple users affected	Single user affected
URGENCY	High	Critical service or system completely unavailable[1]	**P1** Critical	**P2** High	**P3** Medium
	Medium	Service is degraded, possible workarounds[2]	**P2** High	**P3** Medium	**P4** Low
	Low	Minor functions impacted, inconvenience[3]	**P3** Medium	**P4** Low	**P4** Low

[1] High:

- A business-critical system or service is completely unavailable, causing a full stop to work for affected End Users as no alternatives or workarounds area are available.
- A minor Incident which has the potential to escalate into a major one if an immediate action is not taken.
- Reputational risk if the Incident is not resolved quickly.

[2] Medium:

- A business-critical system or service is degraded, or a non-critical system is unavailable. Workarounds or alternative solutions can be used, or work can be deferred in the short term.
- The impact may increase over time or become critical at a certain point, e.g., month-end, or if a market transaction is being planned.
- Potential reputational risk if the issue is not resolved.

[3] Low:

- A service is degraded or some functions unavailable, however, workarounds are available, or work can be deferred.
- The impact will not significantly increase over time.
- No reputational risk implications.

The initial categorisation will be done by the Provider. If requested by the ESM, the Priority Level applied can be adjusted downwards or upwards (e.g., upwards in the case of the ESM Management Board Member being impacted).

If an Incident cannot be resolved quickly and, in any case, in line with the applicable SLR based on its Priority Level, the Provider will ensure that it is escalated to the second level support as described in Section 3.1.1 below. After an Incident has been investigated and diagnosed, and the resolution has been tested, the Service Desk will ensure that the End User is satisfied before the Incident is closed.

The resolution of an Incident may not be within the remit of the Provider and in such cases, the Provider will raise the Incident with the relevant Third Party. The Provider will remain responsible for coordinating and proactively tracking the progress, resolution, and outcome of the Incident with the relevant Third Parties.

Note: there are separate priority levels for Security Incidents as set forth in Section 6.5 below.

Security Incidents Management

Management of Security Incidents (as defined in Section 3.1.1 below) is described in Section 6.5 of these ToR.

2.2.3 Service Requests

The Provider will provide "**Service Request Services"** to the ESM. A Service Request is a formal request for Service from an employee, customer, or vendor. These requests are necessary for initiating a pre-defined and agreed-upon Service action as a normal part of Service delivery. The Provider will fulfil Service Requests, to enable End Users and Third Parties to request and receive Services, to source and deliver these Services, to provide information to End Users about Services and procedures for obtaining them; and to assist with general information, complaints, and comments. The Provider will log and track all Service Requests. The Provider will secure the approval of the ESM before fulfilling Service Requests where needed and agreed with the ESM's Service Delivery Manager.

The Standard Service Requests are listed in "*TOR Annex 7 Service Request Catalogue*".

2.2.4 Problem Management

The Provider will be responsible for problem management at the ESM (the "**Problem Management Services**"). The underlying cause of a Problem is not usually known at the time a Problem record is created and the problem management process is responsible for further investigation.

The Provider will provide Problem Management Services to prevent Problems and resulting Incidents from happening, to eliminate recurring Incidents and to minimise the impact of Incidents that cannot be prevented. Problem Management Services will include diagnosing causes of Incidents, determining the resolution, and ensuring the implementation of the resolution. The Provider will ensure that Problem Management Services also maintains information about Problems and the appropriate workarounds and resolutions. The resolution of a Problem may not be within the remit of the Provider and in such cases, the Provider will raise the Problem with the relevant Third Party. The Provider will remain responsible for coordinating and proactively tracking the progress, resolution, and outcome of the Problem with the relevant Third Parties.

2.2.5 Access Management

The Provider will provide **"Access Management Services"** to the ESM according to Best Industry Practice, as required under the Framework Agreement, and in compliance with ESM Policies and ESM Procedures. The Provider will provide and support access management to provide the rights for the End Users to be able to access a Service or group of Services, while preventing access to non-authorised users. The Provider will consult with End Users, address points of concern and manage confidentiality, availability, and integrity of data accordingly, either by directly changing this with existing rights or by forwarding quality details to Third Parties. The Provider will manage both identity (unique information that distinguishes an individual) and rights (settings that provide access to data and the Services). The Provider will verify identity and entitlement, granting access to the Services, logging and tracking access and removing or modifying rights when status or roles change.

3 Ongoing services

The Provider will provide the following services:

(i) End User Services;
(ii) Network Services;
(iii) Services at the Disaster Recovery site,

on an ongoing basis and shall be deemed to have been commissioned by the ESM to the Provider through the conclusion of the Framework Agreement alone.

3.1 End User Services

The End User Services described in this Section 3.1 cover all production, test and development environments, and any other infrastructure environment that the ESM uses from time to time or requires for its End User Services.

End User Services are End-to-End Services, including back-end systems (e.g., File services, WIFI), and provide qualified users with the infrastructure, the devices (e.g., desktops, laptops, mobile devices), operating environment, and the applications such that the End User is able to:

- Connect to and work within the corporate network;
- Access and use required applications and data;
- Be able to work at anytime from anywhere in a secure way.

The Parties acknowledge that this Section 3.1 is not all-inclusive in describing particular activities, resources or other details necessary for the Provider to perform the End User Services properly. The Provider must provide the End User Services described below as they evolve and change during the term of the Framework Agreement. These changes will include modifying, changing, replacing, supplementing and enhancing the End User Services over time, in terms of any changes that the ESM and the Provider may make to the Framework Agreement and its attachments.

The Provider must ensure it provides the End User Services in compliance with the ESM Policies and ESM Procedures.

The End User Services consist of the following categories of the services:

(xii) Service Desk Services;
(xiii) End User Client Services;
(xiv) End User Application Services;
(xv) Service Asset and Configuration Management Services,

where all these services will be provided by the Service Desk acting as the SPOC.

3.1.1 Service Desk Services

The Provider will provide a single, integrated service desk (the "**Service Desk**"), acting as the single point of IT contact ("**SPOC**") for all relevant queries (Incidents, Service Requests, Standard Changes) for all End Users (including external staff and external offices) and Third Parties (including other providers), through the complete life cycle of a Service Request or an Incident (the "**Service Desk Services**").

"**Incident**" is an unplanned interruption to Service (Service Interruption), or a reduction in the quality of Service.

"**Security Incident**" is an Incident related to IT security for which the Provider is responsible under the Agreement.

"**Service Request**" is a request from an End User for information or advice, or for a Standard Change as set out in ITIL, or for access to a Service.

"**Standard Change**" is a preapproved Change with low impact, low cost and defined procedure as defined in ITIL.

The location of the Service Desk is at the ESM Premises. The ESM will provide, as appropriate for the provision of the Services, IT equipment (excluding mobile devices) and basic software (Windows, 365, ServiceNow) for the Service Desk Members.

The Provider will resolve all Incidents and Service Requests that can be resolved by Service Desk Members as first level support. If second level support is required, the Provider will refer or escalate

to more specialised designated Third Parties or ESM staff, or to the Provider staff responsible for the relevant Service, e.g., in relation to the Network Services, as appropriate.

As per ITIL 4, the responsibility of first level support is to register and classify received Incidents and to undertake an immediate effort to restore a failed IT service as quickly as possible. If no ad-hoc solution can be achieved, first level support will transfer the Incident to expert technical support groups (second level support). First level support also processes Service Requests and keeps End Users informed about their Incidents' status at agreed intervals. Second level support takes over Incidents which cannot be solved immediately with the means of first level support. If necessary, it will request external support, e.g., from software or hardware manufacturers.

The aim is to restore a failed IT Service as quickly as possible. If no solution can be found, the second level support passes on the Incident to Problem Management Services as described in Section 2.3.4 above.

Day-to-day management and support of the ESM's meeting rooms, and associated Equipment is in scope. The Equipment supported include but are not limited to:

- Microsoft Teams and WebEx End User support;
- screen and/or smartboard;
- PC, camera connected to the screens, other periphery (e.g. Poly X70);
- other conferencing solutions deployed in the room (microphones & loudspeakers).

Upon request, the Provider will support VIP meetings with in-the-room presence or with a standby person to support immediately in case of issues.

Key processes, attributes and toolsets for the Service Desk

Service Desk Services include the processes listed in the table below, which also illustrates the attributes and toolsets associated with the Service Desk Services.

Key Processes	Key Attributes	Key Toolsets
SPOC. Service desk operations. Service desk administration. Service Request and ticket management. PC management. End User administration. IMACD administration. Self-help. Planning and Analysis. Exception requests. Support for VIP. Support levels. Conference support.	Single point of contact for all IT Service Requests and Incident reports 24/7. Email/web ticketing capability.	Service Request management tool. Knowledge base and knowledge management tooling. Reporting tools.

The table below outlines the service time and language requirements for the Service Desk Services. All time requirements are expressed in CET (Central European Time) and include the remote support for End Users working remotely, the Brussels Office and ESM Disaster Recovery Site.

Requirement	Language supported by the service desk agent	Time of day (Central European Time)	Days
In-office support	English	07:30 to 19:00	Business Days from Monday to Friday (inclusively)
Out-of-office support	English	24 hours a day	7 days a week

For clarification, in-office support refers to the requirement to have Service Desk Personnel onsite the ESM premises. A list of the ESM holidays is established for each year and will be supplied to the Provider on request; during those holidays only out of office support is required, unless otherwise requested by the ESM.

The ESM has the right to request an extension of in-office support hours to cover exceptional circumstances, including holidays and weekends. Extended in-office support hours fall within the scope of On-demand Services referred to in Section 4 below and therefore will be requested via a Release Order or Work Order.

ESM will grant licences to access the ESM ITSM Tool to the Provider resources allocated to ESM with more than 30% dedication to the ESM.

3.1.2 End User Client Services

This Section further identifies the objectives of and describes the Services that Provider will provide to the ESM as End User client Services ("**End User Client Services**").

The End User Client Services include first level services and support required wherever for servers, desktops and laptops, associated peripherals and other related Equipment (such as tablets) are located.

The purpose of End User Client Services is to maintain the Equipment in good working order with up-to-date Hardware and Software.

IMACD of network printers, End Users' equipment, LAN and WLAN, video conferencing and onsite security devices are in scope.

The physical, onsite part of Mobile Device Management (MDM) is also in scope. The Mobile Device Management (MDM) Services covers smartphones and tablets including provisioning to End Users, Asset management, Incident management, etc., and all actions around configuration setup for individual devices needed to connect to the ESM network.

The Provider will also support a managed printing solution as the onsite counterparty. Large network printers are provisioned and managed by a Third Party and in this regard the provider will be responsible only for first level trouble shooting (e.g., paper jam), listing tickets, monitoring the service, and consumables resupply. The Provider will also be responsible to support (not more than 10) consumer printers at home for the ESM Management Board and a few staff members within a radius of maximum 50 kilometres around the ESM Premises. The Provider will fully support up to 16 local colour desk printers in End User offices.

Key processes, attributes and toolsets for End User Client Services

Key Processes	Key Attributes	Key Toolsets
Desk-side support. Hardware break/fix. Software break/fix first level, ticket ownership and	Telephonic, web, chat, and electronic email submissions and confirmation to End Users.	ITSM Tool. Customer satisfaction survey. ESM IT satisfaction survey.

Key Processes	Key Attributes	Key Toolsets
communication with second level. IMACD within scope of the Framework Agreement. Hardware Asset technology refresh. Support for ESM Sites' Network installation, configuration and maintenance. Printer support and maintenance in ESM Sites. Support for Disaster Recovery Site. Video conferencing support, Mobile devices support and configuration.	Programmed for automated dispatch, escalation and notification based on SLRs. Technical Personnel (on-site or dispatched). Interaction and integration with Service Desk.	Knowledge database and knowledge management.

End User Profiles

The ESM IT End User profiles are largely aligned for Hardware and standard Software. The ESM uses the same hardware and models from VIP profile to standard End User. The ESM relies solely on iPhone and iPads for mobile devices. Regarding Software, all End users have a Microsoft E5 licence and access to OneDrive and SharePoint online.

End User Profile	Profile Definition
Standard End Users	Standard profile covering the majority of ESM staff (in most of the cases using laptops), including remote access services. Hardware: – laptop, desktop – smartphone – tablet – softphone – headset (Bluetooth or cable) – screen with webcam, speaker – docking station, USB hub Access from office and remote
VIP End Users	Approximately 10% of staff are categorised as VIP. Profile for ESM VIP require the highest levels of End User Service. Profile details same as standard End User.
End Users in external offices	End User desks at the Brussels Offices. Profile details same as standard End User.
BCP (business continuity planning) End Users	Subset of the external office profile with special configuration. Hardware: Up to 30 standard laptops in position with screens, keyboard etc., plus 16 pool laptops on standby, and 1 Satellite phone (fixed number to be stored at Disaster Recover Site).
Temporary End Users	Temporary ESM staff given an ESM-owned workstation; Profile details same as standard End User except usually no smartphone or tablet

End User Profile	Profile Definition
Temporary End Users with BYOD (bring your own device)	Temporary staff that bring their own device (e.g., consultants), will be provided with virtual client for office and remote access. Hardware: – screen, webcam, docking station, USB hub optional – no workstation (BYOD only) – tablet optional – smartphone optional – Headset optional
External End Users	Board members, users of SharePoint site etc. Support only for specific web services (e.g., portals). No Hardware Access only to specific Web services (e.g., portals)
Cloud PC profile	End Users without configured ESM computer but with access to a 365 Azure Cloud profile

For Equipment, hardware lifetime is usually three years for laptops, desktops, and iPhones, and four years or more for tablets. The Provider will swap all Equipment at its end of life, unless agreed otherwise in writing (including via e-mail) with the ESM.

Customer satisfaction survey and ESM IT satisfaction survey

The ESM will measure End User satisfaction and ESM IT satisfaction via regular and annual satisfaction surveys. The survey tool will be selected by the ESM.

3.1.3 End User Application Services

This Section further identifies the objectives of and describes the Services that Provider will provide to the ESM as End User application Services ("**End User Application Services**").

End User Application Services include, within the first level support, any services and support required to maintain the PC and server Software, and the standard operating environments (whether this environment is virtualised or not) necessary to run the functions and applications associated with PC tasks and activities, as well as the associated business processes. End User Application Services further include the processes listed in the table below, which also details the attributes and toolsets that the ESM associates with End User Application Services.

These include operating systems, operating environment and applications needed to access and use required applications and data, specifically the ESM's applications that are part of its standard approved desktop computing device images.

The Provider is responsible for providing the relevant security elements as described in Section 6 below in relation to the Services. The Provider is also responsible for applying relevant security elements for Third Parties if an onsite intervention is needed.

Key processes, attributes and toolsets for End User Application Services

End User Application Services include the processes listed in the table below, which also illustrates the attributes and toolsets that the ESM associates with End User Application Services:

Key Processes	Key Attributes	Key Toolsets
Patch management. Self-service portal. Client security services.	Remotely delivered. Testing and provision of images.	Auto discovery tool (various). Electronic Software distribution tool (various).

Key Processes	Key Attributes	Key Toolsets
	Applying packaging roll-out or manual install, distribution of all Software. Integrated with the ITSM Tool. Collaborating with the Third Parties.	Integrated with the ITSM Tool self-service portal.

3.1.4 Service Asset and Configuration Management Services

This Section further identifies the objectives of and describes the Service Asset and Configuration Management Services (**"SACM"**). The Provider will provide the SACM to support the ESM by providing accurate information and control across all Software and Hardware Assets and relationships that make up the ESM's IT infrastructure. The Provider will use SACM to identify, control and account for Assets and Configuration Items ("**CI**"), protecting and ensuring their integrity across the service life cycle. The Provider will also extend SACM to non-IT Assets related to the Services (e.g., laptop bags, TV screens, etc) and to Assets shared with Third Parties.

For Hardware part of SACM, all ESM's IT Equipment is within scope. This includes but is not limited to:

- conference room equipment;
- computers;
- peripheral devices;
- smart screens;
- headsets;
- mobile devices;
- desk phones.

The ESM offers End Users UK, German, Belgium, or Swiss-French keyboards.

The ESM currently uses iPhones, iPads, Jabra headsets, Lenovo laptops, wide screens, desktops. A detailed list of ESM's IT Equipment is attached in "*TOR Annex 5 ESM IT Equipment*".

The ESM will order IT Equipment from its Third Party suppliers and the Provider will be responsible for coordinating the orders, receiving them, preparing and distributing the Equipment and, where applicable, related non-IT equipment, to End Users and keeping an inventory of all IT Equipment, including allocation and warranty expiry.

The Provider will liaise directly with ESM's Third Party suppliers of IT Equipment and related non-IT Assets for repair and maintenance matters. During the term of the Framework Agreement, ESM's Third Party suppliers may change. The ESM will inform the Provider of such changes and provide relevant contact details and procedures to follow.

The Provider will support installation of the operating system and relevant Software as requested by the ESM in alignment with the Third Party providing the image.

Software and Hardware SACM will enable the ESM to gain and maintain control over the physical and contractual aspects of Assets throughout the Asset life cycle. This includes (physical) inventory, product stock management, Asset and Asset value tracking (including depreciation), Asset cascading, Asset disposal and report generation.

The Provider will operate the SACM according to the ESM Software Asset Management policy. The Provider is responsible for reviewing and optimising the Software licence usage and cost on a continuous basis, in direct contact with the End Users and their respective managers.

Key processes, attributes and toolsets for Service Asset and Configuration Management Services

Service Asset and Configuration Management Services include the processes listed in the table below, which also details the attributes and toolsets that the ESM associates with Asset Management:

Key Processes	Key Attributes	Key Toolsets
Physical inventory. Asset tracking. Asset cascading and disposal. Contract management (Warranty, Maintenance and Assets for ESM owned equipment).	Asset management. Integration with other tools.	Physical inventory. Asset inventory. CMDB.

3.2 Network Services

The Provider will operate and administer the ESM network, including provisioning, support, maintenance, management, administration, and troubleshooting (the "**Network Services**"). The Provider will ensure that the network is extremely robust with no single point of failure and maintains a very high security standard. The maintenance of the network must be easily transferable to subsequent provider(s).

The ESM Network Services involve:

- Wide-Area Network (WAN) and Metropolitan Area Network (MAN) (lines provided by Third Party);
- Internet access (lines provided by Third Parties);
- network availability management services;
- network operations and administration;
- Local-Area Network (LAN) including patching, routers, switches, WLAN equipment, etc.;
- Network design and engineering;
- Network support Services for all Services under the Framework Agreement;
- Network system management and troubleshooting (e.g., performance, Problem, Change and capacity monitoring);
- Bandwidth management;
- Protocol usage statistics, e.g., identify top talkers by protocol;
- Working with public carriers and other circuit providers to perform any operations activities, e.g., provisioning, Problem management;
- Managing and maintaining all network computing resources (e.g., Hardware, operating system Software and applications) that are required to provide the Services.

Administration includes activities, such as:

- Managing network configuration: routers, firewalls, Internet Protocol (IP) addresses and related Services and components;
- Asset management, including infrastructure Software licenses;
- Physical (e.g., Equipment) and logical (e.g., IP address change) IMACs.

3.2.1 Wide-Area Network (WAN) and Metropolitan Area Network (MAN) Services

The Provider will ensure that the ESM is able to communicate effectively between the ESM Sites as well as with Third Parties via dedicated lines (WAN and MAN). The Provider will supply WAN and MAN services to include design, monitoring and management of ESM' network (WAN and MAN) that interconnects two or more separate facilities that span a geographic area (**"WAN and MAN Services"**).

The Provider will monitor and report that there is sufficient network capacity and redundancy for the ESM to transmit data both internally and externally as required to meet its business objectives. Transmission facilities include, but are not limited to, point-to-point circuits, dedicated Internet connections, broadband Internet connections and Internet based VPN connections. The Provider will work with public carriers and other providers on behalf of the ESM to ensure delivery and monitoring of WAN and MAN Services. Support of any network Services related work required by designated carriers, to support the ESM network, is considered within the scope of Services. The Provider will be responsible for the WAN and MAN lines, and it is the Provider's responsibility to design, monitor and manage the WAN and MAN networks.

3.2.2 Internet Access Services

The Provider will manage and monitor centralised Internet access to all users of the ESM LAN to ensure undisrupted access to a high-quality Internet access that meets the SLRs.

The Provider will in future propose the best technical solution (centralised access or multi-local, firewalls, proxies) according to cost and performance efficiency.

3.2.3 Managed Local-Area Networks – LAN, WIFI, Eduroam

The Provider will install and maintain all networks and connected equipment to allow End User devices to connect to the ESM resources. This includes the supply and installation of all necessary Hardware, cabling and other Equipment to ensure a high-performance connection both fixed and wireless for all End Users.

The setup and equipment will satisfy the very high security standards of the ESM.

The Provider will:

- Manage the ethernet and WIFI network at the ESM Sites;
- Provide the necessary network equipment to allow End User devices to connect to the ESM cloud infrastructure;
- Provide dedicated switches for the End Users. These switches must be dual attached to core switches to reduce Hardware failure impact and thereby improve continuous Service to all End Users;
- Manage the WIFI: coverage, device connection;
- Secure company WIFI for laptops and mobile devices;
- Provide and manage WIFI for visitors: registering, password management;
- Provide a separate WIFI for the Gym, FM WIFI, Broadcasting room and Board room;
- Provide a dedicated, ad hoc WIFI for special events at the ESM;
- Provide company WIFI connections in the Brussels Office;
- Provide WIFI on demand at the Disaster Recovery Site;
- Support the ESM conference centre with high density of up to 200 people with 2 devices;
- Provide AirPrint: possibility to print documents for End Users connected on WIFI;
- Ensure very high security standards.

A detailed list of current network devices is attached in "*TOR Annex 6 ESM Network Inventory*". The current provider will remove all owned network devices after the end of the contract between the current provider and the ESM (31/12/2025). Hence, it is crucial that the Provider will set up the new network in time to allow for a seamless transition. The ESM requires that the new network set up by the Provider is agnostic, i.e., that it will allow for continued maintenance by a subsequent provider.

The Provider will provide access to Eduroam (EDUcationROAMing), a secure international roaming service for members of the European eduroam Confederation in order to allow End Users from participating academic institutions a secure internet access at any eduroam-enabled institution by

using ESM's WIFI infrastructure (cf. ESM WIFI) with a specific "Eduroam" SSID. As part of it, the Provider will be responsible for, in particular:

- Implementation of a Visitor local area network (VLAN) for eduroam-authenticated End Users,
- Ensuring technical recommendations are implemented as described in the European Eduroam Service definition in accordance with the applicable legislation.

For information, services referred to in this Section 3.2.3 are currently provided via Extreme Networks and UCOPIA. Candidates can propose any other tools fulfilling the requirements.

3.2.4 Network Access Control

The Provider will:

- Provide a network access control solution, ensuring that only authorised End Users can connect known devices to the network;
- Supply a Network Management solution to monitor and control access for all end devices within the ESM network;
- Measure and report the number of identified devices connected to the network;
- Measure and report the number of attempts to connect an unauthorized device to the network;
- Alert IT Security in case of suspicious activity;
- Collaborate with IT Security and Third Parties to ensure the highest level of security.

Network Access Control solutions must integrate with ESM's environment, i.e., be compliant with MS Azure services (e.g. with Microsoft Entra ID to provide authentication integration and Sentinel for log integration). The solutions must cover all ESM Sites.

Depending on the nature of the network and its use, different authentication methods can be used, e.g., device certificates + user credentials, only device certificates/credentials, only user credentials, shared credentials.

Different network access control solutions can be used to accommodate different uses, e.g., one for internal network integrated with Entra ID, another for guest access with captive portal functionality. For information, the existing network access control solution in use at ESM is Extreme Networks (formerly known as Enterasys). Candidates can propose any other tools fulfilling the requirements.

3.2.5 Network Analysis

The Provider will provide a tool to allow deep dive analysis, network utilisation and trend monitoring capabilities, minimum 6 months into the past. The objective is to have a clear view of what operations/processes take place on the ESM network and how the Provider should plan the evolution of the network for future growth.

The Provider will provide:

- Proactive network analysis and trending;
- Monitoring and reporting of End Users, devices, locations, and applications in use;
- Deep packet inspection to understand application usage;
- Reporting for application, End Users, device counts and bandwidth usage;
- Reporting on irregularities to IT security.

For information, the existing tool in use at ESM is Extreme Networks – Analytics (formerly known as PurView). Candidates can propose any other tools fulfilling the requirements.

3.2.6 LAN Segmentation

The Provider will provide a segmented ESM network based on functional groups and information Assets. End Users authorised to access a certain group will belong to one segment. These End Users will not be able to access the network resources belonging to another segment. Additional segments can be added later.

Candidates can propose any tools and setup fulfilling these requirements.

3.3 Services at Disaster Recovery Site

The Provider will ensure provisioning of equipment and associated Services at the ESM Disaster Recovery Site. The DR Site must have an IT environment that can be either in standby mode when not in use or activated when the ESM needs to use the DR Site. While in standby, the IT environment at the DR Site needs to be secure. In case of activation, the Provider needs to ensure working services within 2 hours.

The services to be provided include:

- Network;
- Computers provision and support;
- Software configuration;
- Peripherals;
- Onsite presence to deliver onsite support services during activation, i.e., in case of a disaster or in case of testing.

Specific service elements that are part of regular testing and operations:

- IT disaster recovery tests, implementing recommendations arising from the tests,
- Validation & annual testing.

For the avoidance of doubt, the ESM sources the physical DR Site, including associated physical security services, separately.

3.4 Roles and Responsibilities

"*TOR Annex 8 Roles and Responsibilities"* sets out the general responsibilities of the Parties in relation to the Services referred to in this Section 3.

4 On-Demand Services

On-demand Services can be requested at any time in addition to the Ongoing Services described in Section 3 of this ToR. "**On-Demand Services**" are ESM's requirements associated with the Ongoing Services that arise on an irregular basis only and are ordered by the ESM via a Release Order or a Work Order.

On-Demand Services are divided into Ad-Hoc Services and Project Services as further explained below.

4.1 Ad-Hoc Services

"**Ad-Hoc Services**" are minor, ad-hoc assignments required by the ESM within the scope of the Framework Agreement which do not require complex specifications and require at least two person hours and less than 20 person -days (i.e.,160 person hours) for completion.

If the ESM determines a need for the Ad-Hoc Services, the ESM will provide the Provider with a Release Order, unless the ESM determines, in its sole discretion, that due to the complexity, risk, or any other element of the assignment, a Work Order is required.

Examples of Ad-Hoc Services include:

- Urgent intervention for a large group of End Users at their desk, e.g., for a BIOS update;
- ESM requested, special tasks on weekends such as shutdown of network components for UPS tests;
- Replacement of broken network components due to a water leakage;
- Swapping and reinstallation of computers for a larger amount of End Users, breaking the regular end of life cycle.

Ad-Hoc Services will be provided on time and material basis based on the number of person-hours required for the completion of the requested Ad-Hoc Services and the hourly unit rate applicable for Ad-Hoc Services.

Release Orders for Ad-Hoc Services will be issued in accordance with the procedure set forth in the Framework Agreement and will be based on a Release Order template attached as an annex thereto.

4.2 Project Services

"**Project Services**" or "**Project(s**)" are projects, tasks, or works required by the ESM within the scope of the Agreement that generally require more than 20 person days (i.e., 160 person hours) to complete and due to the risks or complexities involved require more detailed specifications to be agreed between the Parties in the form of a Work Order.

Examples of Project Services include:

- Expansion of the current network to a newly rented part of the ESM Building;
- Swapping and reinstallation of all computers for all End Users within, e.g., 4 months, breaking the regular end of life cycle.

Project Services will be provided on time and material basis based on the number of person-hours required for the completion of the requested Project Services and the hourly unit rate applicable for Project Services.

Work Orders for Project Services will be agreed and entered into by the Parties in accordance with the procedure set forth in the Framework Agreement and will be based on a Work Order template attached as an annex thereto.

5 Transition

5.1 Phase-in

Upon signature of the Framework Agreement, the Provider will be responsible for taking over the Services, as detailed in Section 3 of these Terms of Reference, from the incumbent provider of the ESM (the "**Phase-in**"). During the Phase-in, the incumbent provider will continue to be responsible for delivery of the Services until the handover, the procedure of which shall be set forth in the transition plan referred to below.

For the change of the network components, the list of the current network components, including those that the incumbent provider will remove, at the end of the contract the ESM has with the current provider, is attached in "*TOR Annex 6 ESM Network Inventory*". Another key element for the transition will be the knowledge transfer from the incumbent provider.

The Provider must ensure that all network components installed, and Services provided, are easily transferable to subsequent providers.

The Provider will complete the transition of the Services in a professional, well-planned, and coordinated manner within a maximum of six (6) months of the effective date of the Framework Agreement.

The Provider will be required to play the lead role in the execution of the transition during the Phase-in including planning, coordination, preparation, and facilitation of all required activities to ensure a seamless and successful transition. The Provider commits to a close and constructive collaboration with ESM's IT team and the incumbent provider and to be proactive and organised in ensuring all relevant documentation, knowledge and access credentials are made available to the Provider alongside with any other pre-requisites for the transition completion.

The Provider will develop a detailed and documented transition plan (the "**Transition Plan**" or the "**TP**"), in line with industry standards for such documents, to be supplied to the ESM, which will include but will not be limited to:

- individual tasks and work items to be performed;
- roles and responsibilities of the Phase-in actors, including the ESM IT Division and the incumbent provider;
- tasks and work items scheduling;
- dependencies, critical paths, milestones, risks and related risk mitigation matters;
- liaison and coordination with third parties;
- quality assurance, testing, security, and check lists.

The final TP is to be developed in consultation with the ESM and, if applicable, the incumbent provider and/or Third Party experts arranged by the ESM. The Provider will not implement the TP until the ESM has confirmed its acceptance of the TP in writing.

The Provider must deliver the final TP within one month of the effective date of the Framework Agreement.

The Provider will maintain and update the TP as the Phase-in progresses in order to identify issues, update progress achieved, and record any other subjects agreed with the ESM. Scheduled updates to the TP will be at least on a weekly basis during the Phase-in period.

5.2 Phase-out

At the end of the term of the Framework Agreement, or upon termination of any aspect of the Servies, howsoever arising in each case, the Provider will be responsible for providing transition services to the ESM to ensure the orderly handover of Services to the ESM or another Third Party (the "**Phase-out**"). The Provider will continue to perform the Services until the successful handover the Services to the replacement provider or the ESM, or until successful decommissioning of the Services, as required by the ESM.

The Provider will be required to support the ESM and, if applicable, the subsequent provider in transition of the Services, which will include all relevant assistance as requested by the ESM. As part of such assistance, the Provider may be required to:

- cooperate with the ESM and, if applicable, the subsequent provider by promptly taking all steps required to assist the ESM in completing the Services transition process;
- provide to the ESM such information within Provider's possession or control relating to the Services as is reasonably necessary to enable the ESM to undertake a re-tendering of certain or all of the Services;
- provide the ESM, and, if applicable, the subsequent provider with any information, non-proprietary documentation and data relating to the Services that these parties will need to successfully accomplish the Services transition process;
- transfer of all relevant, non-proprietary knowledge with respect to the Services so that the ESM and, if applicable, the subsequent provider can assume, following the Service transition process, full responsibility for providing the Services without interruptions;

- assess and inform the ESM of security and operational risks pertinent to the Services transition process and possible preventative and curative measures necessary to deal with such risks;
- promptly and orderly conclude all work as the ESM may direct the Provider to do (this may include the documentation of work in progress and other measures to provide an orderly Services transition to the ESM, or, if applicable, the subsequent provider).

For the avoidance of doubt, the Provider will not be entitled to claim any remuneration for the assistance to the ESM and the subsequent provider in transition of the Services as described above.

6 Security Requirements and Responsibilities

The ESM has a zero cyber security risk approach. Accordingly, all Services under the Framework Agreement must incorporate security-by-design underneath, i.e., all underlying IT systems must be properly secured, hardened and maintained.

The Provider will apply security best practices across all the Services. These include (not-exhaustive list):

- usage of encryption at rest and in transit;
- system redundancy;
- zero trust;
- usage of secure communication protocols.

The Provider must assess Services' availability to properly support each Service's availability requirements (Equipment's redundancy will be analysed for each Service and implemented where applicable).

The Provider must manage security of the Services and perform the security activities, referred to in this Section 6, seamlessly, regardless of the technology platform, and at all times ensuring the least disruption possible to ESM's business and the End Users.

The Provider must adhere to the confidentiality, availability, integrity, accountability and traceability requirements of the ESM set out in the Framework Agreement and as further specified by the common security standard ISO 27001 (the "**Security Principles**").

Throughout the entire term of the Framework Agreement the Provider will maintain valid security certifications, e.g., ISO 27001 or equivalent, and exercise all security best practices.

The fees for the provision of the Services include any compensation due to the Provider for complying with security requirements and fulfilling security-related responsibilities.

6.1 Hardening

All IT equipment needed to provide the Services must be hardened, e.g., network firewalls, routers, switches, servers. Hardening is done based the following benchmarks and these benchmarks are listed in order of priority:

(i) Internationally recognised, vendor-independent hardening benchmark, e.g., CIS hardening benchmarks. The ESM prefers that CIS hardening benchmark is used in this step as the global standard and recognized best practice for securing IT systems and data.
(ii) Vendor's guidelines for hardening, or vendor's hardening.
(iii) The Provider will develop hardening guidelines together with the ESM.

If the preferred benchmark does not exist, the next benchmark in the list will be applied.

6.2 Vulnerability management

The Provider will be responsible for vulnerability management and remediation of the Equipment as described further below.

Vulnerability management

The Provider will provide and manage a vulnerability management solution that automates vulnerabilities discovery, reporting and prioritisation by means of a recurring (at least once per month):

- Vulnerability scanning covering the network, Provider's Equipment used in the provision of the Services and any Equipment operating on the ESM network;
- Assessment, which should measure the vulnerability severity based on CVSS version 3 (or its replacement) and accordingly categorise discovered vulnerabilities per CVSS severity levels (Critical, High, Medium, Low).

Note: The initial categorisation of the vulnerability, if requested by the ESM, can be adjusted downwards or upwards.

A vulnerability management solution must be regularly updated to cover for new publicly available vulnerabilities.

The Provider will extract on the 1st Business Day of each month the list of all vulnerabilities. The results, based on the vulnerability severity assessment, will be presented, in the first week of each month, to IT Security in the vulnerability report.

Vulnerability remediation

The Provider will remediate vulnerabilities on all Equipment falling within its responsibility, e.g., Network Services related Equipment and Provider's Equipment used for the Provision of the Services. This refers to vulnerabilities detected by the Provider as a result of Equipment scanning or which the Provider is made aware of otherwise, e.g., as informed by the ESM or Third Parties. As part of the obligation referred to in this paragraph, the Provider must also regularly patch all Equipment's Software.

The Provider will address the discovered vulnerabilities in accordance with minimum SLRs for vulnerability remediation as set forth in "*TOR Annex 9 – SLA*" and will report to IT Security on the status of the vulnerability remediation deployed at agreed intervals. "**Vulnerability Detection Date**" referred to in "*TOR Annex 9 – SLA*" means a day on which a specific vulnerability has been detected by the Provider irrespective of the detection manner, e.g., through the Equipment scanning or information received from the ESM or Third Parties. Information on Vulnerability Detection Date must be included in the vulnerability report referred to earlier in this Section 6.2.

Equipment outside the scope of Provider's responsibility

With regard to vulnerabilities of the Equipment falling outside of Provider's responsibility, e.g., Microsoft 365 or Microsoft Azure, the Provider, acting in its capacity as the first level support, will refer, within one Business Day of vulnerability detection, to designated Third Party responsible for the Equipment in question and IT Security, providing all information regarding the detected vulnerability as may be reasonably required. The Provider will also coordinate and proactively monitor vulnerability remediation passed onto the relevant Third Party and keep IT Security regularly updated.

The fee for the Network Services agreed upon in the Framework Agreement shall be inclusive of any costs associated with vulnerability remediation referred to in this Section 6.2. Accordingly, the Provider will not have any right to claim any additional compensation in consideration of vulnerability remediation.

6.3 Network access control

The Provider will ensure network access control in line with requirements, including but not limited to security, set forth in Section 3.2.4 above.

6.4 Network traffic control

The Provider will provide a solution that enables control over incoming and outgoing traffic of ESM's networks. Traffic needs to be able to be blocked per certain content category (web traffic control) and provide exceptions to that. Blocking must be possible by IP address or fully qualified domain name (FQDN). Network traffic control solution needs to have https decryption capabilities if requested by the ESM. The current solutions for traffic control are Cisco WSA for corporate traffic and Ucopia for traffic on guest networks.

For servers residing in ESM's networks, their access to internet needs to be controlled via a reverse proxy solution.

Traffic between clients, e.g., user laptops, in the same layer 2 segment and between different subnets is by default blocked. The solution must allow whitelisting traffic between clients on the network.

6.5 Incident response

The Provider will provide security incident response service. This is a special case of Incident Management Services, with different Service Level Requirements needed for this special case.

Security Incidents must be managed in order to have the least possible impact on the provided Services (according to the Security Principles set out above) and in accordance with SLTs for *Containment Time – P1 Security Incidents* and *Containment Time – P2 Security Incidents* SLRs set forth in *"TOR Annex 9 – SLA"*.

Security Incidents Priority Levels

(i) Priority Level 1 (S-P1): Incident affecting ESM's critical systems or data, direct impact.

Typical incident categories: denial of services, compromised asset (critical), internal hacking (active), external hacking, virus/worn (outbreak), destruction of property.

(ii) Priority Level 2 (S-P2): Incident affecting ESM's non-critical systems or data, indirect impact.

Typical incident categories: internal hacking (not active), external hacking (not active), unauthorised access, ESM Policies violations, unlawful activity, compromised information, compromised asset, destruction of property (non-critical).

For the avoidance of doubt, there are no P3 and P4 Priority Levels for Security Incidents.

"**Containment Time**" means time during which the Provider must take immediate measures to limit the extent and impact of a Security Incident to prevent its further damage, if any, and spread. As part of Security Incident containment, the Provider must, as a minimum, ensure the following:

- Immediate response:
  - **Isolation:** Disconnecting affected Equipment components from the network to prevent the spread of a Security Incident;
  - **Temporary Measures:** Implementing short-term fixes or workarounds to stop a Security Incident from worsening while a permanent solution, i.e., remediation, is developed.
- Damage Limitation:

- **Preventing Spread**: Ensuring a Security Incident does not affect additional Equipment components, End Users, or data. For example, containing a virus outbreak within an infected segment of the network.
- **Minimizing Impact:** Reducing the overall impact on business operations, such as rerouting network traffic or restricting access to sensitive areas.

– Assessment and Monitoring:

- **Incident Analysis**: Quickly understanding the nature and scope of a Security Incident to apply the most effective containment measures;
- **Ongoing Monitoring**: Continuously monitoring the affected Equipment components and the wider network to detect any signs of a Security Incident spreading or reoccurring.

6.6 Security Operation Centre – SOC

The ESM has an established SOC service supported through Microsoft's Sentinel solution. Solutions that the Provider will use to support their service delivery need to support integration with Microsoft Sentinel for security monitoring. The Provider will need to integrate security logging of all IT solutions with ESM's SOC monitoring solution – Sentinel.

The Provider will cooperate with ESM's SOC team on resolution of any security events and incidents.

6.7 Security Exercise and External / Internal Audit Requirements

The Provider will participate in relevant cyber exercises and any requests for information or reports during external or internal audits, including addressing any recommendations arising out of them.

6.8 Roles and Responsibilities

"*TOR Annex 8 Roles and Responsibilities"* defines the general responsibilities of the Parties in relation to the security requirements referred to in this Section 6.

7 Ticketing

The proper, accurate and timely management and logging of Service Request tickets and Incident tickets is essential to ensure the proper management of End User Services and Service Desk Services and to ensure fees incurred under the Framework Agreement are in line with the commercial terms thereof.

The End Users will be able to report Service Request tickets and Incident tickets in the manner preferred by them which means they will be able to do so via the ESM ITSM Tool as well us using other communication channels used at the ESM, e.g., via Teams (chat and phone) or an email sent to a Service Desk Personnel or to the Service Desk functional email address. For the latter cases, i.e., where the End User does not open a ticket directly, the Service Desk Personnel will open a ticket promptly on their behalf in the ESM ITSM Tool. The Provider may promote the direct use of ESM ITSM Tool among End Users.

The Provider at all times will comply with the following rules throughout the duration of the Framework Agreement:

(i) each Service Request, Incident and Problem must be registered in ESM ITSM Tool as a ticket;

(ii) Ticket Assignment Time must take place within 30 minutes of the notification of the Service Request, Incident or Problem to the Service Desk, regardless of the manner in which the notification was made;

(iii) the Provider must ensure that tickets for the same Service Request, Incident, and/or Problem are not duplicated;

(iv) A "**Closed Ticket(s)**" is a ticket(s) which is fulfilled and can no longer be reopened. Tickets for Service Requests are closed immediately on resolution and cannot be reopened and are therefore immediately classified as "Closed Tickets" once resolved. Tickets for Incidents and Problems can be reopened within 30 calendar days of the initial resolution by the End User who raised the ticket or Service Desk Personnel. For the avoidance of doubt, tickets for Incidents and Problems are only categorised as "Closed Tickets" when they cannot be reopened;

(v) If the subject matter of a ticket for an Incident or a Problem reoccurs within 30 calendar days of an initial resolution of the original ticket, the original ticket must be reopened instead of opening a new ticket;

(vi) Once a Problem is identified, any further tickets raised with respect to that Problem will be dealt with under a single ticket.

(vii) the Provider is responsible for the overall administration of Service Request tickets, Incident tickets, and Problem tickets in the ESM ITSM Tool, i.e., logging (if applicable), tracking, resolution, reporting and closure;

(viii) When forwarding tickets to third parties, the Provider is responsible for ensuring that the ticket contains sufficient and relevant detail to minimise the time to solve it and to reduce follow up questions;

(ix) tickets must be cancelled instead of being closed if, for whatever reason, the subject matter of the ticket is not fulfilled;

(x) tickets are on an individual End User level, i.e., tickets cannot be raised for two or more End Users for End User Services and Service Desk Services. The only exception to this is if an Incident, Problem, or Service Request is not of an individual nature and functionally concerns a group of End Users or the entire ESM, e.g., a network outage for a part of the ESM Building. The same applies if only a single mitigation action is required to solve multiple open tickets at once;

(xi) one ticket covers the entire cycle of a Service Request, Incident, and/or Problem until the Service Request, Incident and/or Problem is resolved irrespective of the Service Request, Incident, or Problem length or complexity. Splitting tickets pertinent to one Service Request (as per *"TOR Annex 7 Service Request Catalogue"*), or, in case the specific Service Request is not listed therein, as per Service Request definition under the Framework Agreement, is not permitted. The preceding sentence applies also to Incidents and Problems accordingly.

The Service Desk Manager will constantly monitor ticket management, proactively pre-empting the occurrence of irregularities and deficiencies. The Service Desk Manager will also develop, in consultation with the ESM, procedures and manuals to support compliance with and implementation of these rules and ensure Service Desk Personnel comply with them.

ESM's Service Delivery Manager will regularly review tickets metrics in the ESM ITSM Tool and, to the extent required, discuss them during Monthly SDR Meetings and ad-hoc meetings.

8 Personnel

8.1 Personnel General Minimum Requirements

The Provider remains at all times responsible and liable for Provider's Personnel.

The Provider will provide all Provider's Personnel considered necessary for the provision of the Services to the ESM, including a dedicated team composed of Key Personnel.

The Key Personnel must include the following roles:

- Account and Contract Manager;
- Service Delivery Manager;

- Asset Manager;
- Service Desk Manager.

All Provider's Personnel (including Key Personnel) will meet individually the following minimum non-exhaustive requirements:

- Be fully capable of performing the duties described in this TOR;
- Be presentable and display a pleasant and appropriate attitude with a customer focused approach;
- Be able to multitask;
- Have good communication skills;
- Good command of written and spoken English.

whereas profile specific requirements are set forth further below in Section 8.2.

The Provider will ensure that Provider's Personnel comply with ESM's security, health and safety policies and guidelines.

The Provider will also ensure that Provider's Personnel provided to the ESM have clean criminal records, all required education, qualifications (including certificates and training), and required previous experience.

The ESM reserves the right to carry out verification, at any time, that the requirements referred to above or profile specific minimum requirements are met. The ESM may also interview any proposed Provider's Personnel resource prior to his/her onboarding in order to assess his/her suitability.

8.2 Profile Specific Minimum Requirements

Account and Contract Manager

The account and contract manager appointed by the Provider will have overall responsibility for directing all of the Provider's activities within the scope of the Framework Agreement and will be vested by the Provider with all necessary authority to act for the Provider in connection with all aspects of the Framework Agreement (the "**Account and Contract Manager**").

The primary role and skills of the Account and Contract Manager are as follows:

Key responsibilities

- Addressing any issue and/or problem faced by the ESM and dealing with complaints;
- Leading and facilitating contractual activities from the Framework Agreement signing through transition and ongoing operations;
- Monitoring compliance with contractual terms and providing recommendations to resolve issues related to non-compliance;
- Identifying and managing fee reductions (in the form of Service Credits), based on performance information as required under the Framework Agreement;
- Working closely with relevant ESM's departments and coordinating discussions on any matters arising out of or in relation to the Framework Agreement, e.g., potential amendments if required, etc.;
- Acting as primary contact for all billing and financial issues;
- Reviewing invoices, ensuring invoicing quality and timeliness and recommending corrective action, if needed;
- Reviewing fee reductions and identifying problem areas and recommending corrective action;
- Be the primary relationship manager between the Provider and the ESM;

- Knowledgeable about the Framework Agreement, including Release Orders and Work Orders falling under it, ESM's other providers and each of those providers and subcontractors' products and services.

Minimum requirements:

- 5 years of experience of running services of a size and scope similar to those of the ESM;
- Experienced in reviewing and editing contracts;
- Excellent written and communication skills in English.

Work Location: This role can be performed offsite.

Service Delivery Manager

Each Party will designate individuals who will be each Party's primary point of contact for all matters relating to the execution of the Services (generally **"Service Delivery Manager"**, for the ESM, the "**ESM Service Delivery Manager**", and for the Provider, the "**Provider Service Delivery Manager**").

Key responsibilities of the Provider Service Delivery Manager:

- Ensure the adequacy of solutions delivered to the ESM's business needs;
- Ensure that the expected quality and level of Services are delivered;
- Coordinate the Service delivery;
- Analyse events and propose corrective and preventive actions in collaboration with ESM's IT operations manager;
- SLRs & SLTs reporting;
- Control SLRs & SLTs indicators and carry out the corrective actions required;
- Organise and lead Service review meetings;
- Maintain up to date knowledge about the Services and any other Third Parties, including their products and services provided to the ESM, which are directly or indirectly involved in service delivery impacting the Services under the Framework Agreement;

Minimum requirements:

- 5 years of experience of running Services of a size and scope similar to those of the ESM;
- Excellent written and communication skills in English.

Work Location: This role can be performed offsite.

Asset Manager

The asset manager assigned by the Provider is responsible for updating and maintaining the correctness of the Hardware and Software inventory in accordance with the respective ESM Policies and ESM Procedures (the "**Asset Manager**").

Key responsibilities:

- **Asset Tracking and Inventory Management**:
  - Maintain an accurate inventory of all Assets, including Hardware, Software, licenses, and related documentation;
  - Use asset management tools and systems to track the location, status, and lifecycle of Assets;
  - Perform regular audits and reconciliations of Assets inventories.
- **Coordination and Deployment**:
  - Ensure that new Assets are deployed efficiently and according to organisational standards;
  - Coordinate with all stakeholders to understand the IT Asset needs and requirements.
- **License Management**:
  - Track and manage software licenses, including renewals, upgrades, and expirations;

- Optimise license usage to reduce costs.

- **Lifecycle Management**:
- Manage the entire lifecycle of IT Assets from acquisition to disposal;
- Develop and implement policies and procedures for Asset lifecycle management;
- Plan and execute the retirement and disposal of obsolete or end-of-life Assets.
- **Financial Management**:
- Analyse and report on the cost of Assets;
- Identify opportunities for cost savings and more efficient Asset utilisation.
- **Compliance and Risk Management**:
- Ensure Asset management practices comply with internal policies and external regulations;
- Identify and mitigate risks related to Assets, such as data breaches, theft, or loss;
- Conduct risk assessments and implement security measures for IT Assets.
- **Vendor Management:**
- Maintain relationships with vendors and service providers;
- Evaluate vendor performance and report issues;
- Coordinate with vendors for maintenance, support, and warranty services.
- **Reporting and Analysis**:
- Generate regular reports on Asset status, usage, and performance;
- Use data analytics to identify trends and make informed decisions about Asset management;
- Provide insights and recommendations for strategic planning.
- **Process Improvement**:
- Continuously assess and improve Asset management processes and tools;
- Implement best practices and industry standards for Asset management;
- Ensure awareness of current Asset management policies and procedures with other stakeholders, including team members.
- **Collaboration and Communication**:
- Collaborate with IT, finance, procurement, and other departments to ensure effective Asset management;
- Communicate Asset management policies, procedures, and updates to relevant stakeholders;
- Serve as the primary point of contact for all matters related to Asset management.

Minimum requirements:

- 5 years of experience of running Asset management of a size and scope similar to those of the ESM;
- Excellent written and communication skills in English.

Work Location: This role is a full-time requirement and needs to be performed onsite a minimum of four Business Days a week.

Service Desk Manager

The service desk manager, assigned by the Provider, is responsible for the execution, management, and performance of the Service Desk at the ESM (the "**Service Desk Manager**").

Key responsibilities:

- **Team Management**:
- Supervise and lead the Service Desk Personnel;
- Assign tasks and manage workloads to ensure efficient handling of Service Requests and Incidents;
- Foster a positive team environment.

- **Service Delivery**:
- Ensure timely and effective resolution of Service Desk tickets;
- Monitor Service Desk performance metrics, such as response time, resolution time, and customer satisfaction;
- Implement and maintain service level agreements (SLAs) and key performance indicators (KPIs).
- **Process Management**:
- Develop, implement, and continuously improve Service Desk processes and procedures;
- Ensure adherence to best practices and industry standards for IT service management;
- Maintain efficient processes for Incident, Problem, Change, and Service Request management.
- **Customer Service**:
- Maintain a high level of customer service and ensure a positive End User experience;
- Address escalated customer issues and complaints promptly and effectively;
- Gather feedback from the End Users to identify areas for improvement.
- **Incident and Problem Management**:
- Oversee the identification, categorisation, and resolution of Incidents;
- Implement Problem management processes to identify and resolve root causes of recurring issues;
- Coordinate with Third Parties to ensure effective Incident and Problem resolution.
- **Review and Analysis**:
- Review Service Desk performance with metrics and trends;
- Analyse data to identify patterns, trends, and areas for improvement;
- Present findings and recommendations to the ESM IT Division.
- **Technology Management**:
- Manage Service Desk tools and technologies, such as ticketing systems and remote support tools;
- Ensure the Service Desk tools are configured and used effectively;
- Stay updated on emerging technologies and recommend improvements to the Service Desk infrastructure.
- **Training and Knowledge Management**:
- Ensure training programs for Service Desk Members to enhance their technical and customer service skills;
- Maintain a knowledge base of common issues, solutions, and best practices;
- Ensure knowledge base articles are updated and accessible to both Service Desk Members and End Users.
- **Vendor and Stakeholder Management**:
- Manage relationships with Third Party vendors and service providers when required;
- Coordinate with vendors for escalated support issues and ensure compliance with SLRs & SLTs;
- Communicate with stakeholders to understand their needs and ensure the Service Desk meets their expectations.
- **Strategic Planning**:
- Develop and implement strategies to improve Service Desk operations;
- Participate in IT strategy and planning;
- Plan for future Service Desk needs, including staffing, technology, and process enhancements;
- Identify cost-saving opportunities and optimise resource allocation.

Minimum requirements:

- 5 years of experience of running a Service Desk of a size and scope similar to the one of the ESM;
- Excellent written and communication skills in English.

Work Location: This role is a full-time requirement and needs to be performed onsite a minimum of four Business Days a week.

Service Desk Personnel

The members of the Service Desk, assigned by the Provider to perform the Services, are responsible for the execution of Service Desk related Services at the ESM.

Key responsibilities:

- **Technical Support**:
- Provide first-level support for Hardware, Software, and network issues;
- Troubleshoot and resolve technical problems reported by End Users;
- Escalate complex issues to higher-level IT support when necessary.
- **End User Assistance**:
- Answer queries and provide guidance on using IT systems and applications;
- Assist End Users with password resets, software usage, and system navigation.
- **Incident Management**:
- Log and track Incidents and Service Requests in the ticketing system;
- Prioritize and manage multiple Incidents and Service Requests simultaneously;
- Follow up with the End Users to ensure issues are resolved satisfactorily.
- **System Maintenance**:
- Perform routine maintenance on computer systems and networks;
- Update software and apply patches to ensure system security and performance;
- Monitor system performance, identify and report potential issues.
- **Documentation**:
- Maintain accurate records of all Incidents and Service Requests;
- Document solutions and create knowledge base articles for common issues;
- Update IT procedures as needed.
- **Communication**:
- Communicate effectively with the End Users to understand their issues and needs;
- Provide regular updates to End Users on the status of their requests;
- Collaborate with other stakeholders to resolve issues and improve services.
- **Hardware Support**:
- Set up and configure new Hardware, including computers, printers, and peripherals;
- Diagnose and correct Hardware faults, follow repair process;
- Manage inventory of IT Equipment and supplies.
- **Network Support**:
- Assist with network connectivity issues;
- Support the setup and maintenance of network equipment such as routers and switches;
- Ensure network security by monitoring access and updating configurations as needed.
- **Customer Service**:
- Maintain a high level of customer service and professionalism;
- Address End User concerns empathetically and efficiently;
- Ensure End User satisfaction with IT services and support.
- **Continuous Improvement**:
- Stay updated with the latest changes to the infrastructure and best practices;
- Provide feedback to improve IT support processes and tools.

Minimum requirements:

- 2 years of experience at another Service Desk of a size and scope similar to the one of the ESM;
- Good written and communication skills in English.

Work Location: This role is a full-time requirement and needs to be performed onsite a minimum of four Business Days a week. There must always be Service Desk Personnel onsite at any given time during the In-Office support hours. The ESM reserves the right to increase the requirement for onsite presence of Service Desk Personnel during the term of the Framework Agreement at its own discretion.

8.3 Personnel availability

The Provider will be required to identify upfront backup resources/proxies for all Key Personnel with, at minimum, the same level of experience and skill set required for each of those key roles in the event of an unplanned temporary absence (sick leave for example) in order to minimise gaps in carrying out those responsibilities.

The Provider shall also maintain a sufficient number of Service Desk resources in order to avoid any understaffing which may have an adverse impact on quality of the Services and lead to violation of Service Levels Requirements.

8.4 Personnel retention and replacement

The Provider will use commercially reasonable efforts to keep the fluctuation of Provider's Personnel to a low level. The Provider will ensure that the replacement of Provider's Personnel, however arising, will not disrupt the performance under the Framework Agreement.

The ESM may, at its own discretion, prior to and during the course of the Framework Agreement, request the replacement of any Provider's Personnel, without any justification.

Any potential change to the composition of the Key Personnel requested by the Provider will be an exception and only permissible if a Key Personnel resource:

(i) resigns from their employment;
(ii) is unable to work because of illness or another matter beyond their control for more than four (4) weeks;
(iii) is removed following a request of the ESM in accordance with this Section 8;
(iv) is reasonably dismissed by the Provider with good cause.

Should a replacement of a Key Personnel resource become necessary, ESM's Service Delivery Manager must be notified at least 60 calendar days in advance except in situations arising outside Provider's control.

In the event the Provider is required to replace any Provider's Personnel, for any reasons, the Provider will take immediate steps to identify and provide an alternative resource meeting the requirements applicable for the specific role, to ensure availability and continuity of the Services. The Provider will ensure the replacement Provider's Personnel is sufficiently trained during an adequate handover period which facilitates all required knowledge transfer, to ensure the replacement resource/s can be immediately operational and perform at least at the same level as their predecessor. Proposals for new Provider's Personnel must be reviewed and approved in writing (including via e-mail) by the ESM and the Provider cannot commence the use of the new Provider's Personnel until an approval is provided by the ESM in this manner.

In all cases where an adjustment in Provider's Personnel is requested by the Provider and approved in writing (including via email) by the ESM, or where the ESM requires such an adjustment, the Provider will be responsible for the cost of the transition from one resource to another and, for the avoidance

of doubt, any and all other costs associated with such adjustment in Provider's Personnel. As such, knowledge transfer and potential overlap between Provider's Personnel is Provider's responsibility and will not be charged to ESM.

The ESM will not be involved in the management of Provider's Personnel.

9 Service Level Requirements

The purpose of service level management is to ensure that all operational services and their performance are measured in a consistent and professional manner.

"*TOR Annex 9 – SLA*" attached to these Terms of Reference describes Service Level Requirements ("**SLRs**") and corresponding Service Level Targets ("**SLTs**") applicable to the Services. SLRs and SLTs referred to in the preceding sentence are minimum requirements of the ESM in this regard. Candidates are invited to propose in their technical proposals higher SLTs and/or additional SLRs with associated SLTs.

The Provider and the ESM will conduct a review of "*TOR Annex 9 – SLA*" prior to the completion of the Phase-in, within one (1) year of the commencement of the Framework Agreement, and, at the ESM request, at any point during the term of the Framework Agreement. Any changes to "*TOR Annex 9 – SLA*" must be agreed by both parties in writing. For the avoidance of doubt, the ESM will not be under any obligation to agree to any changes to the SLRs and corresponding SLTs.

In addition to the SLRs, the Provider will perform the Services:

(i) in a manner ensuring a high level of accuracy, completeness, efficiency, quality, responsiveness, and timeliness;
(ii) promptly, using reasonable skill and care and in a professional and workmanlike manner; and;
(iii) in accordance with any other performance standards specified in the Framework Agreement.

The achievement of the SLTs by the Provider may require the coordinated, collaborative effort of the Provider with Third Parties. The Provider will provide a single point of contact for the prompt resolution of all SLR breaches and all failures, in order to provide high quality Services to the ESM, regardless of whether the reason for such SLR breach, or failure to provide high quality Services to the ESM, was caused by the Provider or not.

9.1 Service Level Measurement

The Provider will measure its performance against the SLRs in accordance with *"TOR Annex 9 – SLA"* and will provide a detailed, comprehensive report of its performance against the SLRs during each applicable reporting period (the "**Monthly SLR Report(s)**").

If there are any SLRs for which the measuring tools and methodologies have not been determined in *"TOR Annex 9 – SLA"* and the Provider fails to propose a measuring tool for such SLR that is acceptable to the ESM prior to the date upon which the Provider shall be responsible for such SLR, such failure shall be deemed a breach of the respective SLR until the Provider proposes and implements such acceptable measuring tool.

The Provider will provide to the ESM, as part of Provider's Monthly SLR Reports, a set of softcopy reports to verify Provider's performance and compliance with the SLRs. The Provider will agree the format of these reports in advance with the ESM Service Delivery Manager. The Provider will provide the ESM with detailed supporting information for each Monthly SLR Report.

The ESM's failure to analyse and enforce SLRs shall not be deemed a waiver of such performance standards.

The following rules shall apply at all times throughout the duration of the Framework Agreement:

(i) Services will be delivered, and Service Level Targets will be measured, using the local time in Luxembourg, i.e., CET, as seasonally adjusted for summer time (CST);

(ii) If the Provider fails to report appropriately against the Service Level Requirements, the ESM reserves the right to treat this as a failure to meet SLRs;

(iii) In case of a breach of a Service Level Requirement, Service Credits will be calculated by the ESM based on the mechanisms described in the sections below;

(iv) If the Provider anticipates that it may not be in a position to comply with an SLR, the Provider will immediately inform the ESM in writing via email, inclusive of the rationale and circumstances surrounding the anticipated non-performance, any temporary solutions or work around plans, an indication on timing when it can comply in the manner intended and other relevant details as may be reasonably warranted under the circumstances;

(v) If the Provider fails to meet a SLR, the Provider will immediately start the agreed escalation process, define and implement corrective actions and provide a root cause analysis to the ESM without undue delay;

(vi) For purposes of calculating actual uptime/downtime and Availability, any period of downtime that is the result of scheduled time required to perform system maintenance (for example, preventive maintenance, system upgrades, etc.) will not be included, provided that such time has been mutually agreed between the Parties and is scheduled so as to minimize the impact to the ESM's business. The Provider will maintain Availability during such periods to the extent reasonably possible.

9.2 Service Credits

If the Provider fails to meet the relevant SLTs as set out in "*TOR Annex 9 – SLA*", the ESM may claim the corresponding Service Credits. The Parties agree that the Service Credits reflect the diminished value of the Services as a result of the Service Provider's failure to provide the Services in accordance with "*TOR Annex 9 – SLA*".

The Service Credits will be treated separately and will be cumulative for the different SLRs.

The Service Credits calculated for the applicable monthly period will be discussed during the Monthly SDR Meeting, regarding that period. The ESM may assess whether the Service Credits are not applicable based on the outcomes of the Monthly SDR Meeting. If the Service Credits are applicable, the procedure described in the Framework Agreement will apply.

The maximum monthly cap on Service Credits payable for failure to meet any or all of the SLTs will be no more than 15% of the total monthly service fees, save for months in which a quarterly or annual SLT is measured in which case the maximum monthly cap on the Service Credits payable will be 18%.

Payment of Service Credits is without prejudice to and will not limit any other rights the ESM may have under the Framework Agreement. Service Credits will not have any impact on any claim for damages (including claims related to SLTs breaches) by the ESM.

10 Reporting

The Provider will be required to prepare and submit Monthly SLRs Reports in the manner specified in Section 9.1 above. The deadline for the submission of the Monthly SLRs Reports will be agreed by the Parties in the Framework Agreement or otherwise, with a view to ensure a timely organisation of the Monthly SDR meetings.

The Provider will also report to IT Security on vulnerabilities detected (each month as further specific in Section 6.2 above) and on vulnerability management activities (at pre-agreed intervals), with the format and exact content to be agreed with the ESM.

In addition to the above reports, the Provider may be required to prepare and submit to the ESM other types of reports, including but not limited to:

- General reports pertaining to its activities and performance under the Framework Agreement;
- Any ad-hoc reports, which should be prepared in the manner and within the commercially reasonable time limits, as instructed by the ESM. Such reports may cover any Service and contractual related matters and be required for legal, regulatory or compliance purposes, proper contract management (including budgetary matters) or for any other reasons as determined at ESM's sole discretion.

11 Meetings

The Provider Service Delivery Manager and the ESM Service Delivery Manager will hold, following the receipt of the monthly SLR Report for the respective month by the ESM, monthly service delivery review meetings ("**Monthly SDR Meetings**") during which they will discuss the Monthly SLR Report for the last month as well as any other ongoing and ad-hoc matters in connection with Provider's performance under the Framework Agreement. Monthly SDR Meetings will be also attended by other representatives of either Party to the extent the Parties deem it appropriate, e.g., in the view of the specific meeting agenda.

Monthly SDR Meetings will be scheduled by the Provider Service Delivery Manager. The Provider Service Delivery Manager will also prepare an agenda for such meetings and will send it to the ESM's Service Delivery Manager at least three Business Days in advance of the monthly SDR meeting to allow a reasonable opportunity to prepare for the monthly SDR meeting and for ESM's Service Delivery Manager to add any items to the agenda as necessary.

In addition to monthly SDR meetings, the ESM may, at any time, organise or require the Provider to organise any additional meetings, with or without notice, i.e.,:

- Ad-hoc meetings, to discuss any matters regarding the execution of the Framework Agreement;
- Escalation meetings, to discuss any matters regarding the execution of the Framework Agreement, which, at the ESM opinion, require escalation or the upfront involvement of both parties' senior representatives.

Ad hoc meetings shall be attended by the ESM Service Delivery Manager, as accompanied by other ESM's representatives in case of a need, and the Provider Service Delivery Manager, as accompanied by other members of Provider's Personnel as requested by the ESM Service Delivery Manager or otherwise found appropriate by the Provider Service Delivery Manager. The same applies with regard to escalation meetings with the proviso that senior representatives of both Parties shall attend such meetings as well.

The Provider Service Delivery Manager shall take minutes of all meetings and share them via SharePoint with the ESM Service Delivery Manager within one week of the date of the meeting.

All meetings will be held remotely unless otherwise requested by the ESM.

12 Governance

The main contact persons on the Provider side shall be the Account and Contract Manager and the Provider Service Delivery Manager. Their responsibilities, include, but are not limited to, the overall management and administration of the Framework Agreement and coordination of the provision of the Services.

The main contact person on the ESM side shall be ESM Service Delivery Manager.

The Account and Contract Manager and the Provider Service Delivery Manager will facilitate an open and transparent working relationship with the ESM and ensure consistent communication with regard to all aspects of the Framework Agreement execution and the provision of the Services.

Proper, efficient and timely communication is of the essence to achieve the successful cooperation and therefore aside from reporting and meetings requirements set forth in the preceding Sections of this TOR, the Provider and the ESM will use the collaboration and instant messaging tools to facilitate day-to-day management and cooperation under the Framework Agreement. Currently the ESM uses Microsoft Teams as both a collaboration and instant messaging tool.

The ESM-approved formal reporting and communication processes and structures will be mutually agreed upon and established in order to manage the delivery of the Services from the Provider in an efficient and effective manner. These will be documented, modified and updated on an ongoing basis, to reflect changes to the business and operational relationship, by the Provider and approved by the ESM.

The Provider must maintain and keep, in the agreed manner, available to the ESM Service Delivery Manager:

- an up-to-date delivery organisation chart mapped to the defined Key Roles along with current contact information;
- an escalation matrix with current contact information for the Provider's senior representatives for issues relating to any aspect of the Framework Agreement execution and the provision of the Services, including but not limited to the following domains: account management, Service performance, compliance, financial and contractual.

Contact information will include the role, email and telephone information.

***

Annexes to the Terms of Reference:

1) TOR Annex 1 Definitions
2) TOR Annex 2 Amount of Incidents January 2020 to July 2024
3) TOR Annex 3 Amount of Requests January 2020 to July 2024
4) TOR Annex 4 Request Distribution Type January 2023 to December 2023
5) TOR Annex 5 ESM IT Equipment
6) TOR Annex 6 ESM Network Inventory
7) TOR Annex 7 Service Request Catalogue
8) TOR Annex 8 Roles and Responsibilities
9) TOR Annex 9 – SLA