

1. Overview

This TOR Annex 8 *Roles and Responsibilities* identifies the roles and responsibilities of the Parties in relation to the Ongoing Services falling within the scope of the ToR, i.e.:

- (i) End User Services referred to in Section 3.1 of the ToR;
- (ii) Network Services referred to in Section 3.2 of the ToR;
- (iii) Services at the Disaster Recovery Site referred to in Section 3.3 of the ToR,

as well as in relation to:

- (iv) Service Integration management processes referred to in Section 2.3 of the ToR; and
- (v) Security Requirements referred to in Section 6 of the ToR.

This annex is intended to identify either party roles and responsibilities comprehensively. Nevertheless, the ESM and the Provide are aware that this document is not all-inclusive in describing particular activities, resources or other details necessary to ensure the proper execution of the Framework Agreement. Accordingly, to the extent not determined hereunder or as otherwise may be required by the ESM in the specific circumstances, each party roles and responsibilities shall be determined in accordance with the following:

- If any Provider’s roles and responsibilities are not specifically described hereunder or elsewhere in the Framework Agreement but are required for the proper performance of the Services, whether Ongoing or On-demand, Service Integration management processes or Security Requirements, and are an inherent part thereof, or a necessary sub-part included within them, then Provider’s such roles and responsibilities shall be deemed to be implied by and included within the scope of the Provider’s roles and responsibilities to the same extent and in the same manner as if specifically identified hereunder or elsewhere in the Framework Agreement;
- Provider’s roles and responsibilities shall be deemed to be implied in the manner ensuring that the Services are performed, and the Framework Agreement is executed in line with Best Industry Practice and in conformity with ITIL based practices;
- the ESM at all times retains the exclusive right and authority to develop the ESM's IT strategy and architecture, and to determine, alter and define any or all the ESM's requirements and operational and/or business processes and procedures.

2. Roles and Responsibilities

2.1. End User Services

2.1.1. Service Desk Services

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Service Desk general roles and responsibilities	Provider	ESM
Set up and run the service desk, use the ITSM tool to document, track and manage End User request for Services, inquiries and Problem notifications.	Responsible	
Proactively perform the morning check with agreed tasks from 07:30 to 8:30 on business days to ensure issues are recognised early	Responsible	

Provide a single point of contact and coordination for all Incident reports and Service Requests, such as IMACD in the Services supported under the terms of the Framework Agreement.	Responsible	
Provide expert First level assistance to inquiries on the features, functions and usage of Hardware and Software.	Responsible	
Resolve and close Problems where appropriate or identify and escalate.	Responsible	
Manage the root cause analysis (RCA) process on recurring Problems covered by the Framework Agreement.	Responsible	
Perform First level support where required for administration services such as creating, changing and deleting user accounts.	Responsible	
First level support of the Microsoft Office Suite (excluding macros).	Responsible	
First level support for Software requests.	Responsible	
First level support for the End Users, including redirection to other points of contact, third parties where appropriate and supporting the End User to resolve the issue.	Responsible	
First line of support of security issues (e.g., unlock password, diagnosis of access issues).	Responsible	
First line of support of teleworking issues (remote access).	Responsible	
First level support for unified communication (iPhones, and iPads, Microsoft Teams, etc.)	Responsible	
First level support for Software issues.	Responsible	
Diagnosis of Hardware issues.	Responsible	
Troubleshooting of printers and scanners.	Responsible	
Provide key service desk staff to support the ESM at the disaster recovery site in case of a disaster.	Responsible	
Single Point of Contact (SPOC)	Provider	ESM
Provide SPOC call-in access for all service desk services.	Responsible	
Provide for multiple alternative communications channels, including voice messages, Teams chat, email and ITSM tool.	Responsible	
Record and redirect non-Service Desk IT service Incidents and Service requests.	Responsible	
Service Desk Operations	Provider	ESM
Develop and document operational procedures that meet requirements and adhere to defined Service Desk policies.	Responsible	
Review and approve operational procedures created by the Provider.		Responsible
Receive, track, answer and resolve End User and technical staff calls.	Responsible	
Coordinate IMACD, including all IT End User Service Equipment.	Responsible	
Provide first level assistance for software applications.	Responsible	
Provide first level Problem identification, recording, escalation, resolution and closure process for all topics under the Framework Agreement.	Responsible	
Manage critical events according to the agreed SLRs.	Responsible	
Service Desk Administration	Provider	ESM

Develop and document Service Desk administration procedures that meet End User requirements and adhere to defined Service Desk policies.	Responsible	
Review and accept the Service Desk administration procedures.		Responsible
Track, manage and report the Service Desk utilisation.	Responsible	
Provide escalation contact list(s) for recipient contacts.		Responsible
Maintain and provide escalation contact list(s) for all services (including Third Party providers).	Responsible	
Issue broadcasts or other notices to provide status updates as required for planned and unplanned events.	Responsible	
Provide End Users with an online/portal access to Service requests and Incident reports.		Responsible
Develop and execute procedures for conducting End User satisfaction surveys.	Responsible	
Review and approve procedures for conducting End User satisfaction surveys.		Responsible
Maintain a continuous improvement program of service desk services using metrics.	Responsible	
Work with own and third party operational and technical staff, as well as recipients, to identify solutions that minimise the need to call the Service Desk (such as additional End User training, self-help opportunities and root cause analysis).	Responsible	
Review and approve identified solutions that minimises the need to call the Service Desk.		Responsible
Coordinate and make available environment documentation (such as network configuration and Standard ESM Software List).	Responsible	
Service Request and Ticket Management	Provider	ESM
Identify and describe priorities, response and resolution targets for Service Calls and Requests of differing impacts.		Responsible
Provide the ITSM tool to enable the provider to document, manage and track all Incidents, Service Requests, Problem reports, etc.		Responsible
Develop procedures to receive and respond to recipient calls for service according to defined prioritisation and resolution targets. Ensure that response to requests is based on priority and impact rather than the method used to notify the Service Desk (by telephone, email, Teams chat, direct input to Service request system by End Users or other ways).	Responsible	
Review and Accept procedure to receive and respond to recipient calls.		Responsible
Review and Accept procedure for the escalation of Incidents.		Responsible
Right to audit the categorisation and prioritisation process and its accuracy.		Responsible
Resolve Incidents within prescribed time limits, if possible; otherwise, escalate to appropriate second level support resources.	Responsible	
Identify Problem characteristics and root cause.	Responsible	
Categorise, prioritise and log all Incidents, inquiries, Problems and Service Requests correctly in the ticket system that arrive at the Service Desk.	Responsible	

Monitor Incidents and Service Requests and escalate per policies and procedures until resolution and End User satisfaction, also if assigned to third party tickets.	Responsible	
Verify acceptance of services by contacting the End User to confirm results and level of satisfaction.	Responsible	
Ensure that recurring Problems that meet defined criteria are reviewed using root cause analysis processes.	Responsible	
Ensure that inventory and configuration management records are updated to reflect completed Service request (IMACD and others).	Responsible	
Provide necessary input to End User satisfaction surveys.	Responsible	
Provide End Users with an optional satisfaction survey for every case opened.		Responsible
Collect and report on customer satisfaction regarding case resolution.	Responsible	
PC Management	Provider	ESM
Recommend and develop policies for the use of remote-control tools for maintenance and troubleshooting.	Responsible	
Review and Approve policies for the use of remote-control tools for maintenance and troubleshooting.		Responsible
Diagnose Problems using remote-control capability and, when possible, implement corrective actions to resolve Problems in scope of the agreement. If resolution is not possible, escalate accordingly.	Responsible	
Use remote-control tools to manage and enforce compliance with standards.	Responsible	
Assist in enabling the enforcement of compliance to standards and the appropriate optimisation at the desktop.	Responsible	
End User Administration	Provider	ESM
Develop and document requirements and policies regarding End User administration in scope of the Framework Agreement (e.g., for Oracle).	Responsible	
Review and Approve requirements and policies regarding user administration.		Responsible
Coordinate as necessary with other specialised areas and suppliers to manage End User accounts for systems outside the scope of the Framework Agreement.	Responsible	
IMACD Administration	Provider	ESM
Receive and track requests for IMACD.	Responsible	
Confirm the requirements and scope, acquire recipient approval of the IMACD request for services covered by this Framework Agreement or forward the request to the respective Third Party.	Responsible	
Contact the End User and schedule an appropriate, agreed time for the work to take place in for services under this Framework Agreement.	Responsible	
Verify completion of IMACD by contacting the End User to confirm satisfaction for the services performed.	Responsible	
Self-Help	Provider	ESM
Identify requirements for self-help capabilities.	Responsible	
Suggest and Implement self-help capabilities that enable End Users to perform self-service for Services covered under this agreement	Responsible	

Monitor, review and report on the effectiveness of self-help capabilities and use.	Responsible	
Develop recommendations for and implement improvements to self-help capabilities.	Responsible	
Review and Approve improvements to self-help processes.		Responsible
Exception Requests	Provider	ESM
Develop and document exception request procedures.	Responsible	
Review and Approve the Provider exception process.		Responsible
Document exception requests in trouble ticket system.	Responsible	
Provide request status to requestor when approved.	Responsible	
Planning and Analysis	Provider	ESM
Approve Service Desk solutions and expense/SLRs.		Responsible
Perform operational planning for Service Desk capacity and performance purposes.	Responsible	
Perform analysis of the environment, including acquiring management team feedback, to identify the appropriate sets of skills, training and experience needed by Service Desk staff.	Responsible	
Recommend Incident management, reporting standards and policies.	Responsible	
Report on Service Desk statistics and trends as requested (such as Service Request volumes and trends by types of End Users).	Responsible	
Report on trends in Service Requests indicating the most common issues reported by End Users	Responsible	
Right to audit results and operations periodically.		Responsible
Provide online/portal access to Service Desk reports.	Responsible	
Provide remote access support.	Responsible	
Support for VIP End Users	Provider	ESM
Ensure sufficient support capacity to serve VIP End Users with priority.	Responsible	
Support Levels	Provider	ESM
Provide First level support for Microsoft 365.	Responsible	
Escalate to Level 2 support, when required.	Responsible	
Ensure timely communication from the third-party providers to the ESM by passing on provided information.	Responsible	
Assist third-party providers in incident resolution by providing requested and available information and/or by performing requested actions.	Responsible	
Ensure that information forwarded to Third-Parties has sufficient detail to minimise additional follow-up questions.	Responsible	
Conference support	Provider	ESM
Provide technical assistance for the start of a conference call when requested.	Responsible	
Provide ongoing technical standby assistance for a VIP conference call or event when requested.	Responsible	
Support ESM's internal events with the setup of the inhouse conferencing equipment (e.g., speaker, mixer, mics, mobile screens) when requested.	Responsible	

2.1.2. End User Client Services

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Desk-Side Support	Provider	ESM
Break/fix Hardware and Software support, including troubleshooting at the desktop for Problem determination.	Responsible	
Resolve Problems with long-term fix - if the Problem cannot be resolved within the service-level time frame, implement an alternative route.	Responsible	
Identify and resolve user Hardware/workstation Problems.	Responsible	
Provide End User support and Incident resolution.	Responsible	
Provide End User training on new installations and answer “how-to” questions during that training.		Responsible
Coordinate with Third Party providers to resolve Hardware and Software Problems, as required.	Responsible	
Install and test replacement parts.	Responsible	
Coordinate and support physical relocations.	Responsible	
Perform client reporting including feedback on Problem tracking and request tracking.	Responsible	
Support projects where the Service Desk support or knowledge is needed.	Responsible	
Break/fix Hardware and Software support.	Responsible	
Provide support for End User’s specific projects and needs.	Responsible	
Initiate, update and close Problem tickets in the ITSM.	Responsible	
Client reporting - includes feedback on Problem tracking, Service Request tracking, project updates and chargeback information, and technology budget planning.	Responsible	
Coordinate support to meet relocation schedules and needs of End Users.	Responsible	
Install and test required replacement and spare parts.	Responsible	
Provide Problem resolution and move, add, change (“MAC”) support to the End User’s point of business/work.	Responsible	
Provide trouble shooting and Problem resolution and MAC for all transmission and telecommunications devices required for the End User’s needs.	Responsible	
Provide End User instructions and guidance on how to use system features and services for services under the Framework Agreement.	Responsible	
Provide technical support and advice to resolve problems and provide solutions for new requirements.	Responsible	
Handling Incidents which require an on-site intervention, also for third parties (roaming technician, remote hands support).	Responsible	
Hardware and Software Break/Fix	Provider	ESM

Resolve in-scope Hardware Problems and coordinate and support resolution of Software and hardware Problems with Third Parties where required.	Responsible	
Interface with Hardware and Software providers or other Third Parties for planning and Problem resolution.	Responsible	
Perform regular maintenance on distributed Hardware, which require such periodic maintenance.	Responsible	
Provide maintenance for authorised user Hardware that require such periodic maintenance.	Responsible	
Perform appropriate adjustments, repairs and replacements necessary to restore equipment and/or Software operation and performance to manufacturer's specifications.	Responsible	
Maintain required inventories of spares, sufficient capacity must be kept on site to avoid business disruption. Communicate shortages.	Responsible	
Interface with manufacturers and third-party providers for technical assistance.	Responsible	
Interface with Hardware providers and return defective Hardware for repair or replacement, obtain repairs or replacements.	Responsible	
IMACD	Provider	ESM
Re-order and cascade new and used Equipment.	Responsible	
Perform MAC requests and update the work management system.	Responsible	
Coordinate the installation of PCs, peripherals and LAN-based Equipment.	Responsible	
Set up or support Third Parties with the security, file access and other administrative procedures associated with moves.	Responsible	
Determine End Users' requirements on an exceptional basis whenever the End User requests an out-of-scope service.	Responsible	
Move workstations, screens, and other IT equipment as required.	Responsible	
Coordinate activities around IT IMACD and proactively act upon physical desk environment wherever possible.	Responsible	
Install non-network Software for End Users in local Sites.	Responsible	
Review and Approve installation of non-network Software for End Users.		Responsible
Ensure that connectivity issues are addressed for installations.	Responsible	
Consult with End users to identify and clarify their needs on an exceptional basis whenever the End User requests an out-of-scope service.	Responsible	
Assess infrastructure capabilities to satisfy End Users' needs.	Responsible	
Review and Approve assessment of infrastructure capabilities.		Responsible
Identify incompatibilities among the End users' applications, needs and the established infrastructure.	Responsible	
Consult and collaborate with third-party providers to satisfy End Users' needs.	Responsible	

Obtain approvals from the ESM to proceed with selected implementations.	Responsible	
Review and Approve requests for selected implementations.		Responsible
Coordinate activities around IT IMACD including national and international moves.	Responsible	
Prepare and submit required communication to initiate orders for equipment, Software and third-Party services.	Responsible	
Initiate, update and close work requests in the work management system.	Responsible	
Coordinate with facilities for MACs that require infrastructural modifications.	Responsible	
Install and remove audio/video conferencing Equipment as required, including lift and shift service for large screens (smartboard, TV, etc.). Includes installation of fixation for the hardware.	Responsible	
Review and Approve movement of audio/video conferencing equipment.		Responsible
Establish and change security passwords for access to transmission systems or other systems under the Framework Agreement for maintenance and MAC operations.	Responsible	
Establish or organise secure initial passwords for End User access or take appropriate alternative action when End Users have lost their passwords. Consult on good behaviour for passwords.	Responsible	
Plan and schedule moves according to the requests of the ESM and coordinated with the ESM facility management services.	Responsible	
Review and Approve schedules moves.		Responsible
Order, receive and provide all required equipment, materials and third-party provider services to implement IMACs.	Responsible	
Coordinate installation and the set-up of Equipment, cables, outlets and all other Hardware required for implementing IT IMACD together with the ESM facility management services.	Responsible	
Review and Approve installation of Equipment, cables, outlets and all other Hardware.		Responsible
Coordinate and support installation of network systems in the ESM facilities by third-party providers in coordination with the ESM's Facility Management services.	Responsible	
Test completed MACs and verify acceptance by an End User.	Responsible	
Document changes to inventory use and configuration.	Responsible	
Perform End User notifications to single End Users for routine activities.	Responsible	
Prepare and perform End User notifications for significant changes or other announcements, e.g., via Intranet, email or other means.	Responsible	
Approve End User notifications for significant changes or other announcements, e.g., via Intranet, email or other means.		Responsible
Installations, moves and configuration of local printers and scanners.	Responsible	

Perform office moves within Business Hours of up to 3 workstations per day as part of the standard Service delivery.	Responsible	
Technology Refresh	Provider	ESM
Recommend and establish technology roles and responsibilities (“TR&R”), life cycle management policies, procedures and plans appropriate for the support of the ESM’s business needs.	Responsible	
Approve TR&R policies, procedures and plans in accordance with the change and release management process.		Responsible
Manage, maintain and update, as necessary, approved TR&R policies, procedures and plans.	Responsible	
Perform the tasks required to fulfil TR&R plans.	Responsible	
Provide management reports on the progress of TR&R plans.	Responsible	
Periodically review the approved TR&R implementation plans to ensure that they properly support the ESM business requirements.	Responsible	
Support for External Offices and Disaster Recovery Site	Provider	ESM
Undertake 2 visits/year to the Disaster Recovery Site and ensure proper functioning of services at the Disaster Recovery Site the Provider is responsible for.	Responsible	
Preventive maintenance and reporting on network printers in collaboration with third-party provider.	Responsible	
First level support for break & fix of network printers	Responsible	
Office extensions, re-fittings and moves.	Responsible	
Maintenance for equipment (firmware upgrades, configuration updates, outdated equipment replacement).	Responsible	
Manage inventory of IT Equipment in each office.	Responsible	
On-site troubleshooting for issues that can’t be handled remotely.	Responsible	
End Users first level support, e.g. for video conferencing related issues.	Responsible	
On-site support (IMACD), including network printers, network devices and security.	Responsible	
Support and troubleshoot deployment of ESM image in the disaster recovery site.	Responsible	
Monthly deployment of changes and updates to Hardware and support for deployment for Software in the disaster recovery site to ensure identical configuration to the main site (i.e., the ESM Premises), including on site testing if required.	Responsible	
First level Printer Support and Maintenance, also in External Offices, Disaster Recovery Site and for Management Board home printing	Provider	ESM
Shipping toners & equipment parts replacement.	Responsible	
Scheduling urgent interventions.	Responsible	
Create a report each time an intervention is performed.	Responsible	

Troubleshoot printer issues that can be checked remotely before deciding if an urgent intervention is necessary.	Responsible	
Video Conferencing Support	Provider	ESM
Monitor the audio/video conferencing (VC) feedback from End Users and act upon	Responsible	
Monitor availability and quality of data lines used by video conferencing within the ESM.	Responsible	
Test the VC devices when necessary	Responsible	
Support VIP video conference calls with in-room or nearby physical presence when required (up to 20h per month)	Responsible	
IMACD support for all Equipment	Responsible	
First level support for all ESM Video conferencing	Responsible	
Newcomers (i.e. new End Users) setup and training support (Wiki page).	Responsible	
MDM - Mobile Device Life Cycle Management	Provider	ESM
Communicate order estimates and cascade new and used equipment.	Responsible	
Ensure proper configuration and profile settings, including all actions establishing proper connectivity.	Responsible	
Ensure that connectivity issues are addressed for installations.	Responsible	
Explain product usage, limitations and maintenance.	Responsible	
Verify products functionality via a standard test.	Responsible	
Manage Asset inventory and monthly reporting.	Responsible	
Backup device data when replacing.	Responsible	
Provide unrestricted access to the mobile devices.		Responsible
MDM - Hardware and Software Break/Fix	Provider	ESM
Problem diagnosis and support including iOS apps limited to apps considered for professional use.	Responsible	
Installing, in a timely manner, all critical firmware updates to the products, where applicable.	Responsible	
Coordinate Software and Hardware related problems activities, resolve or hand over to third parties.	Responsible	
Return faulty Hardware to appropriate source and obtain repairs or replacements.	Responsible	
Communicate with manufacturers and Third-Party providers for technical assistance.	Responsible	
Interface with Hardware vendors and return defective Hardware for repair or replacement.	Responsible	
MDM - General Mobile Device Management Services	Provider	ESM
First level of support for 3rd party mobile telephony services.	Responsible	
Management of SIM Card requests to 3rd party and SIM card inventory.	Responsible	

Testing new firmware or updates.	Responsible	
----------------------------------	-------------	--

2.1.3. End User Application Services

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Self-service Portal	Provider	ESM
Ensure the up to date content of the End-user Front-end of the ITSM tool by providing feedback and suggestions to the ITSM maintenance team.	Responsible	
In the self-service portal, provide an approval workflow allowing the designated ESM End Users (e.g., first-line management) to approve or reject the End Users' requests manually or automatically based on the logic agreed upon with the ESM.		Responsible
Patch Management	Provider	ESM
Keep devices up to date: Review, test and apply patches relevant for services under this agreement.	Responsible	
Install or support the install of patches (also for Third Party supplier) which need to be started locally, in a seamless way, considering ESM's Change management needs, including acquiring required organisational approvals.	Responsible	
Provide reporting on patching status to the ESM for services under this ToR.	Responsible	
Client Security Services	Provider	ESM
For all aspects of the service, ensure compliance with the ESM's security policies and standards and report on deviations.	Responsible	
All Software and Hardware components running on End User devices and servers need to be fully functioning and have up-to-date security Software (antivirus, firewall, encryption, etc.). Report on deviations.	Responsible	

2.1.4. Service Asset and Configuration Management Services

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Physical Inventory	Provider	ESM
Maintain an inventory of replacement parts for Hardware maintenance.	Responsible	
Maintain a distributed spare parts inventory, as required to meet SLRs.	Responsible	
Provide periodic reports on spares inventory	Responsible	
Audit inventory accuracy and storage security internally.	Responsible	
Maintain spare equipment and components in an appropriately controlled environment.	Responsible	
Management and distribution of paper, toners and cartridges for printers, also in external offices.	Responsible	

Management of the stock of paper, cartridges and toners.	Responsible	
Asset Tracking	Provider	ESM
Track inventory assets and equipment. Proactively replace equipment at the end-of-life period.	Responsible	
Keep a current database of the location and configuration data associated with each Asset in the ITSM tool.	Responsible	
Produce regular Asset Management reports and make them available on the intranet.	Responsible	
Update and maintain an Asset inventory database in the ITSM tool and End User computing component configuration charts that include, e.g., manufacturer, model, serial number, asset identification number, asset location, purchase date, beginning of life, end of life, invoice information, price, ownership information, configuration information, Software information, mission-critical information, maintenance information and history and the current status of the item, if applicable.	Responsible	
Asset Cascading and Disposal	Provider	ESM
Store on the ESM site the equipment removed from active service until redeployed in an organised, structured way.	Responsible	
Maintain inventory of all End User computing equipment prior to disposal, and issue updates to the CMDB regarding removal.	Responsible	
Review and Approve updates to the inventory upon receipt.		Responsible
Dispose of Equipment no longer required in compliance with the Best Industry Practice and provide a certificate of destruction.	Responsible	
Document changes to inventory use and configuration.	Responsible	
Support the donation of equipment through the ESM 'buyback' scheme. The ESM offers staff to buy laptops, desktops, iPhones and other hardware items at the of the end-of-life period. These items need to be set back to factory default, categorised and handed out to staff as directed by the ESM.	Responsible	
Contract Management (Warranty, Maintenance and Assets for ESM owned equipment)	Provider	ESM
Ensure that all warranty data is entered correctly.	Responsible	
Prepare and submit any warranty-covered rebate paperwork, as appropriate.	Responsible	
Conduct parts management and monitoring for warranty and out-of-warranty Equipment.	Responsible	

2.2. Network Services

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Roles and responsibilities	Provider	ESM
Order and expedite LAN circuits, network Equipment and Services.	Responsible	
Document and maintain documentation for all networks.	Responsible	
Configure LAN (hardware, software) prior to installation.	Responsible	

Document router configuration files and IP addressing schemas.	Responsible	
Develop and document network provisioning requirements and policies.	Responsible	
Provide capacity planning assistance to develop network resource requirements projections to increase the volume of data to transfer or to satisfy new needs e.g., Voice over IP, Multimedia sharing, new sites extensions.	Responsible	
Single point of contact for the ESM Network: coordinate ordering and inventory management of network circuits from other providers.	Responsible	
Ensure that all new circuits, devices and software provisioned are included in configuration management documentation.	Responsible	
Conduct technical tests before and after migration/activation.	Responsible	
Provide the ESM with an interface for monitoring the network and related activities/services in read only mode. This interface will include different views like an overall view of the network with indicators such as status, activity, performance, bandwidth, etc.	Responsible	
Ensure that Availability requirements are included when requirements are collected when designing new network systems and Services to support business End Users.	Responsible	
Execute End User requirements gathering and analysis when new network systems and services are being defined to ensure that network Services and systems are designed to deliver the required SLRs (availability required by the business).	Responsible	
Create Availability and recovery design criteria to be applied to new or enhanced infrastructure design.	Responsible	
Participate in creating Availability and recovery design criteria to be applied to new or enhanced network infrastructure system and services design.		Responsible
Coordinate with the network service support and service delivery management personnel from the ESM and third-party providers to research, review and assess Availability Issues and optimisation opportunities.	Responsible	
Define Availability measures and reporting requirements for the network infrastructure and its components that underpin a new or enhanced network Service as the basis for an SLR agreement that reflect business, End User and network support organisation requirements.	Responsible	
Participate and cooperate with the ESM in defining SLRs and reporting requirements.	Responsible	
Provide LAN connectivity contained in the service environment.	Responsible	
Provide wireless LAN (Wi-Fi) connectivity in the ESM's Sites, including a Guest- Wi-Fi solution.	Responsible	
Develop and document network administration requirements and respective policies and procedures.	Responsible	
Develop/document procedures for network administration that meet requirements and adhere to defined policies and procedures.	Responsible	
Approve network administration policies and procedures.		Responsible
Perform day-to-day network operations and administration activities.	Responsible	

Manage network devices in accordance with the ESM's Policies and Procedures, including security oversight and change management.	Responsible	
Maintain IP addressing schemes, router configurations, routing tables, virtual private network configurations, etc.	Responsible	
Manage End User accounts as needed for access and maintaining network resources, such as logon user-id and password maintenance.	Responsible	
Maintain/provide audit information, including access, general logs and application logs, in accordance with the ESM's security policies.	Responsible	
Ensure that network administration activities are coordinated through defined change management processes.	Responsible	
Develop and document requirements and policies for network monitoring and Incident and Problem management.	Responsible	
Approve requirements and policies for network monitoring and Problem management.		Responsible
Develop and document network monitoring and Problem management procedures, including escalation thresholds, that meet requirements and adhere to defined policies.	Responsible	
Approve network monitoring/Problem management procedures.		Responsible
Provide/implement tools for monitoring network devices/traffic.	Responsible	
Implement measures for proactive monitoring and self-healing capabilities to limit network outages.	Responsible	
Monitor network per SLRs.	Responsible	
Identify network problems and resolve in accordance with incident and Problem management Services, policies, procedures.	Responsible	
Provide on-site staff at organisation facilities, as required, to perform maintenance and Problem resolution activities.	Responsible	
Coordinate resolution of circuit problems with Third Parties, including public carriers, Internet providers and city/county affiliates using the network.	Responsible	
Establish a comprehensive Network Capacity Management planning process.	Responsible	
Define, develop and implement tools that allow for the effective network capacity monitoring/trending of network infrastructure, applications and network components.	Responsible	
Identify and communicate future business requirements that will alter network capacity requirements.		Responsible
Provide input where needed for all network capacity planning activities.		Responsible
Continually monitor network resource usage to enable proactive identification of capacity and performance issues.	Responsible	
Capture trending information and forecast future ESM network capacity requirements based on ESM-defined thresholds.	Responsible	
Assess Incidents/Problems related to bandwidth usage.	Responsible	
Recommend changes to network capacity to improve service performance.	Responsible	
Assess impact/risk and cost of network capacity changes.	Responsible	
Approve network capacity related recommendations.		Responsible

Maintain network capacity levels to optimise use of existing network resources.	Responsible	
Ensure adequate network capacity exists within the network environment to meet SLR requirements taking into account daily, weekly and seasonal variations in network capacity demands.	Responsible	
Validate asset utilisation and capital efficiency based on a report provided by the Provider.		Responsible
Perform Service Equipment tuning to maintain optimum performance in accordance with change management procedures.	Responsible	
Manage Service component resources (e.g., devices and traffic) to meet defined availability and performance SLRs.	Responsible	
Provide regular monitoring and reporting of Service component performance, utilisation and efficiency.	Responsible	
Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance.	Responsible	
Develop and deliver improvement plans as required to meet SLRs.	Responsible	
Implement improvement plans and coordinate with Third Parties as required.	Responsible	
Provide technical advice and support to the application maintenance and development staffs as required.	Responsible	
Provide IT Rooms and racks for on premise equipment.		Responsible
Provide structured cabling for End User devices and on-premise equipment *from the built in sockets box on the floor to the patch panel in the IT Rooms.		Responsible
Maintain the floor plan indicating where the built-in sockets box on the floor are located.		Responsible
Provide and maintain a resilient electrical power supply infrastructure.		Responsible
Provide and maintain grounding and bonding for electrical safety.		Responsible
Provide and maintain the air conditioning equipment.		Responsible
Control relative humidity.		Responsible
Control room temperature.		Responsible
Provide and maintain the leak detection system(s).		Responsible
Provide and maintain the fire detection and fire suppression system(s).		Responsible
Provide and maintain managed physical access to the IT Room(s).		Responsible
Provide and maintain managed physical access to the rack(s).	Responsible	
Provide the requirements to implement Third-Party provider equipment.		Responsible
Cleaning of facilities.		Responsible
Design the organisation of equipment in the racks and take into account the electrical capacity planning (ideally at 80% per rack).	Responsible	
Keep IT rooms clean and remove packaging and other materials.	Responsible	
Install and maintain the Provider's equipment hosted in the racks.	Responsible	
Maintain the inventory of the equipment by racks location.	Responsible	
Inform the ESM for new equipment prerequisites (space and power).	Responsible	
Define and maintain the Provider's IT Room policy and ensure it's applied by the Provider's teams.	Responsible	

Participate on the changes impacting the equipment hosted in the technical IT Rooms.	Responsible	
Maintain the patching of the End Users' devices between the LAN switches and the patch panels and between the End Users' devices and the built in sockets box (Provide LAN cables, cables inventory and labels, uninstall and decommission unused equipment).	Responsible	
Develop network design, engineering and security testing and integration procedures that meet requirements and adhere to Best Industry Practice for WAN and LAN (including wireless access on the ESM locations).	Responsible	
Approve network design engineering, security testing and integration procedures for WAN and LAN.		Responsible
Prepare network design, engineering and security plans and schedules to support new and enhanced applications, architectures and standards for WAN and LAN. Ensure the network design is provider-agnostic.	Responsible	
Review and Approve network design, engineering and security plans and schedules for WAN and LAN.		Responsible
Review and Approve the scheduling of all changes to the network environment.		Responsible
Coordinate with the ESM and affiliated entities, and other providers, as required.	Responsible	
Provide a network that is performant and meets the availability requirements as well as the quality of service expectations set out in this Framework Agreement and the SLRs.	Responsible	
Detect and resolve all (Service impacting) Problems/Incidents and meet any SLRs, specifically the time-to-resolve of P1 and P2 Incidents).	Responsible	
Supply additional capacity and/or utilisation reporting to the ESM where required to avoid a negative impact on service provision and quality.	Responsible	
Provide a network that is flexible in growing or downsizing of the ESM.	Responsible	
Implement a network capacity buffer to allow for flexibility in network extension, so that the ESM's business is not constrained via routine activities such as adding individual staff or additional systems. Examples of such a buffer would include, but are not limited to, additional available ports or additional bandwidth.	Responsible	
Ensure that security is built into the network at all stages and levels from the initial design to the day-to-day operation and management.	Responsible	
Optimise the use of network resource to improve performance and quality without inflating the operational cost through capacity planning, and network optimisation (efficient design, network virtualisation, quality of service benchmark, monitoring).	Responsible	

2.3. Services at the Disaster Recovery Site

As identified in the table *Support for External Offices and Disaster Recovery Site* set forth in Section 2.1.2. above and elsewhere in this annex where roles and responsibilities with regard to the Disaster Recovery Site are referred to.

2.4. Service Integration management processes

2.4.1. Change Management

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Change Management Roles and Responsibilities	Provider	ESM
Provide templates and supporting information for the authorisation of Changes, and to supply the other service management processes with information on planned and ongoing Changes.	Responsible	
Review and Approve templates and supporting information for authorisation of Changes.		Responsible
Filter out requests for Change, which do not contain all information required for assessment or which are deemed impractical.	Responsible	
Verify if the priority of the proposed Change was correctly set by the initiator, and to determine the adequate level of authority to Approve or reject the request for IIL Change.	Responsible	
Authorise, adjust or reject an urgent request for Change as quickly as possible. This process is invoked if normal Change Management procedures cannot be applied because an emergency requires immediate action.		Responsible
Authorise or reject a proposed Change as well as to ensure a preliminary scheduling and incorporation into the change schedule.		Responsible
Authorise or reject a proposed Change as well as to ensure a preliminary scheduling and incorporation into the change schedule.		Responsible
Agree a preliminary schedule for Change implementation and to transfer responsibility for Change deployment to project management and release management.	Responsible	
Review and Approve schedule for such Change implementation.		Responsible
Assess the course of the Change implementation and the achieved results, in order to verify that a complete history of activities is present for future reference, and to make sure that any mistakes are analysed and lessons learned.	Responsible	
Review and Approve above described Change implementation assessment.		Responsible
Update the CMDB and ITSM tool (ticket status, details, etc.)	Responsible	

2.4.2. Event Management

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Event management Roles and Responsibilities	Provider	ESM
Set up and maintain the mechanisms for generating meaningful events and effective rules for their filtering and correlating (event management processes and procedures).	Responsible	
Review and Approve event management processes and procedures.		Responsible
Filter out events, which can be ignored, and to assign categories to events indicating their significance	Responsible	

Interpret the meaning of an event and select a suitable response.	Responsible	
Check if events have been handled appropriately and may be closed. Make sure that event logs are analysed in order to identify trends or patterns, which suggest corrective action must be taken.	Responsible	

2.4.3. Incident Management

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Incident Management Roles and Responsibilities	Provider	ESM
Provide and maintain the tools, processes, skills and rules for an effective and efficient handling of Incidents.	Responsible	
Review and Approve Incident Management processes and procedures.		Responsible
Record and prioritise or reprioritise the Incident with appropriate diligence, in order to facilitate a swift and effective resolution and prevent more incidents for other End Users.	Responsible	
Solve Incidents by providing first-level support within the agreed time schedule as set out in “ <i>TOR Annex 9 – SLA</i> ”, thus enabling fast recovery of the Service, where necessary with the aid of a work-around. As soon as it becomes clear that first-level support is not able to resolve the Incident itself or when target times for first-level resolution are exceeded, transfer the Incident to a suitable group within second-level support.	Responsible	
Solve Incidents within the agreed SLRs as set out in “ <i>TOR Annex 9 – SLA</i> ”, thus enabling fast recovery of the service, where necessary by means of a work-around. If required, involve specialist support groups or Third Parties. If the correction of the root cause is not possible, create a Problem record and transfer error-correction to Problem Management. As soon as it becomes clear that first-level support is not able to resolve the Incident itself or when target times for first-level resolution are exceeded, transfer the Incident to a suitable group within second-level support.	Responsible	
Solve P1 and P2 Incidents, which cause serious interruptions of business activities with greater urgency, enabling fast recovery of the Service, where necessary by means of a work-around. If required, involve specialist support groups or the Third Party. If the correction of the root cause is not possible, create a Problem record and transfer the error-correction to Problem Management. As soon as it becomes clear that first-level support is not able to resolve the Incident itself or when target times for first level resolution are exceeded, transfer the Incident to a suitable group within second-level support.	Responsible	
Submit the Incident record to a final quality control before it is closed, thus making sure that the Incident is actually resolved, and that all information required to describe the Incident's life cycle is supplied in sufficient detail. In addition to this, record findings from the resolution of the Incident for future use.	Responsible	
Continuously monitor the processing status of outstanding Incidents and introduce countermeasures as soon as possible if SLRs are likely to be breached.	Responsible	

Inform End Users of Service failures as soon as these are known to the Service Desk, so that End Users are able to adjust themselves to interruptions. Proactively inform End Users to reduce the number of inquiries by End Users. Distribute other information to End Users, e.g., security alerts.	Responsible	
Supply Incident-related information to the other service management processes and Third Parties, thus making sure that that improvement potentials are derived from past Incidents.	Responsible	
Provide training and knowledge scripts to support Incident Management. Update the knowledge base to solve faster or avoid incidents in the future.	Responsible	

2.4.4. Service Requests

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Request fulfilment Roles and Responsibilities	Provider	ESM
Accept and register End User requests (including but not limited to request for information, or advice, or for a standard ITIL Change or for access to a Service, to reset a password, or to provide standard Services for a new End User). If necessary, pass the request on to the respective Third Party.	Responsible	
Provide Service Request status information upon registered End User demand. The information must consist of a message containing the present status of a Service Request and all relevant details.	Responsible	

2.4.5. Problem Management

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Problem Management Roles and Responsibilities	Provider	ESM
Coordinate Problem Management Services across providers.	Responsible	
Constantly monitor outstanding Problems with regards to their processing status, so that where necessary corrective measures may be introduced.	Responsible	
Record and prioritise Problems with appropriate diligence, in order to facilitate a swift and effective resolution - both reactively and pro-actively.	Responsible	
Identify the underlying root cause of a Problem and initiate the most appropriate and economical Problem solution. If possible supply a temporary work-around.	Responsible	
Ensure that - after a successful Problem solution - the record and prioritise the Problem contains a full historical description, and that related 'known error' records are updated.	Responsible	
Review and Approve Problem resolution and closure.		Responsible
Ensure that the other ITIL service management processes, Third Parties as well as IT management are informed of relevant outstanding Problems, their processing-status and existing workarounds.	Responsible	

Provide and keep Problem Management knowledge base in ServiceNow up to date. Relate to knowledge management service process.	Responsible	
Provide Service improvements when SLRs and other requirements under this Agreement are not met.	Responsible	

2.4.6. Access Management

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Access management Roles and Responsibilities	Provider	ESM
Ensure that the catalogue of user roles and user role access profiles is still appropriate for the Services offered to End Users, and to prevent unwanted accumulation of access rights.		Responsible
Process and complete requests of the ESM to add, change or revoke access rights, and to make sure that only authorised End Users are granted the right to use a Service. If the request cannot be performed by the Provider directly, forward to the respective Third Party. Ensure quality of the requests to minimise back and forth iterations and delays for End User.	Responsible	

2.5. Security Requirements

Notes: Approve = Approval by email or other electronic means; Accept = Acceptance according to the Acceptance Procedure set out in the Framework Agreement

Security general roles and responsibilities	Provider	ESM
Implement critical and major security patches and bug fixes in a timely fashion with the least disruption possible.	Responsible	
Comply with Security Requirements and Responsibilities in line with ESM's business needs and technical requirements.	Responsible	
Define onsite security requirements, standards, policies and procedures for the ESM.		Responsible
Comply with the ESM standards, regulations and policies as set out in Policies and Procedures.	Responsible	
Conform to changes in laws, regulations and policies.	Responsible	
Report performance against SLRs.	Responsible	
Coordinate all changes to the onsite security components which the Provider must maintain to comply with Security requirements and which may affect the SLR of any Service. Support all other changes.	Responsible	
For onsite components, provide timely creation, updating, maintenance and provision of all appropriate projects, project time and cost estimates, technical specifications, management documentation and management for all security related Project as further specified in the Work Order. .	Responsible	
Report Security Incidents to the ESM in accordance with ESM policies.	Responsible	
Resolve Security Incidents in accordance with the SLRs set out in TOR Annex 9 – SLA. .	Responsible	

Install security patches on all IT equipment which is within the scope of the Provider's responsibility.	Responsible	
Install, configure, document, operate, maintain and support (including any needed troubleshooting activities) all Onsite Equipment.	Responsible	
Act as a technical advisor for the ESM on all security topics and emerging technologies and/or threats.	Responsible	
Troubleshoot, and if needed implement correction(s), on all issues/Incidents related to remote access to the ESM's onsite network.	Responsible	
Regularly and proactively review the configuration of security onsite IT equipment to remove obsolete settings and/or exceptions (typically unused firewall rules, obsolete exceptions in whitelists, etc.).	Responsible	
Manage the relationships with various third-party providers on support aspects including management of RMA (Return Material Authorisation) if requested by the manufacturer.	Responsible	
Maintain an up-to-date set of operational documentation of all onsite IT equipment (installation manual, configuration manual, users' manual).	Responsible	
Ensure the decommissioning of any security devices (including the wiping of any ESM-specific and/or personal data if relevant).	Responsible	
Troubleshoot, and if needed implement correction(s), on all issues related to corporate security gateways (connectivity problems, dynamic routing and/or quality of service issues, etc.).	Responsible	
Provide 24/7 on-call services for both technical Incidents and/or cyber-attacks. In particular, in case of major security Incident, ensure immediate remote and/or on-site intervention to ensure efficient containment.	Responsible	
Process any security Incident reported including immediate containment, remediation and/or escalation if necessary.	Responsible	
Troubleshoot, and if needed implement correction(s), on all issues related to the inter-connection of the ESM Premises and its remote offices.	Responsible	
Manage (create/delete) high privileges accesses (administrator accounts) on all network Equipment, laptops, desktops following the least privilege principle.	Responsible	
Ensure that ESM data stored on the Provider's Equipment is separated from other client's data	Responsible	
Notify designated ESM personnel of all severity P1, and P2 security incidents.	Responsible	
Contain, diagnose and remediate security incidents for all in-scope Hardware warranty and non-warranty devices.	Responsible	
Identify and stop the traffic from the WAN of any infected locations based on the security Incident impact assessment.	Responsible	
Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed/resolved Incident.	Responsible	
Security Incident Management	Provider	ESM
Establish criteria for IT Security Incident management support requirements.	Responsible	

Identify and stop the traffic from the WAN of any infected locations based on the security Incident impact assessment.	Responsible	
Identify and classify Security Incident severity level characteristics and handle according to agreed-upon Incident response procedures.	Responsible	
Contain and remediate Security Incidents, using remote control capability wherever possible and with End User approval, and disconnecting once complete and, when possible, implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved Incidents).	Responsible	
Track security Incident resolution progress through to final closure and record/update Incident record status as appropriate.	Responsible	
Notify designated ESM personnel of all severity P1, P2 security incidents.	Responsible	
Records of all tickets and the resolution of those tickets for the life of the contract and provide reporting and trend capabilities through ESM's ticketing system.	Responsible	
Close out Security Incidents that were resolved satisfactorily.	Responsible	
Provide Security Incident management reporting to the ESM.	Responsible	
Fully cooperate with the ESM and Third Parties in the investigation, remediation and recovery from Security Incidents.	Responsible	