

43. SOC Management

43.1 Introduction

Ref	Level	Owner	Description
43.1.1	L3	Supplier	The Supplier shall ensure the Security Operations Centre (SOC) operates as an integral part of the Authority's retained Service Integration (SI) function. The Supplier shall ensure it is a key partner within the Authority's end to end IT Service and amongst other things shall be responsible for the Security Operations Centre.
43.1.2	L3	Supplier	The Supplier shall ensure the Security Operations Centre operates 24 x 7.
43.1.3	L3	Supplier	The Supplier shall ensure the Security Operations Centre covers the technical scope outlined in the Technical Framework Document.
43.1.4	L3	Supplier	Where existing Authority toolsets are in operation, the Supplier shall use, or implement an active interface with, the toolsets.
43.1.5	L3	Supplier	The Supplier shall contribute its internal technology and innovation disciplines to the Authority to bring innovation and industry best practice to the Authority's Security Operations Centre solution.
43.1.6	L3	Supplier	The Supplier shall contribute its internal technology and innovation disciplines to the Authority to bring continuous improvement to the Authority's Security Operations Centre solution.

43.2 General

Ref	Level	Owner	Description
43.2.1	L3	Supplier	The Supplier shall work with the Authority to establish, maintain and enhance SOC Processes, governance and tools that support the Suppliers' end to end responsibility and enable it to provide consistent management, coordination and communication of the delivery of the Services across the supply chain.
43.2.2	L3	Supplier	The Supplier shall, in connection with the provision of the SOC services, maintain and provide the Authority with such supporting documentation and records as the Authority may reasonably require in order to verify the Supplier's compliance with all applicable Policies, Processes and service obligations.
43.2.3	L3	Supplier	The Supplier shall co-operate with and promote joint working between the Supplier, the Authority, and the Authority's Other Suppliers where activities require a multi-party approach.
43.2.4	L3	Supplier	The Supplier shall adhere to the Authority's governance framework.
43.2.5	L3	Supplier	The Supplier shall attend regular meetings, at least monthly, with the Authority and the Authority's Other Suppliers to identify, analyse and give recommendations for continuous service improvement opportunities such as, service interaction volume reduction or increases, productivity, trends in top issues/ requests received and/or Security Operations Centre service offering enhancements.
43.2.6	L3	Supplier	In agreement with the Authority, the Supplier shall promote process efficiency and data quality consistency and the SOC Processes shall be automated wherever there is the opportunity to do so. The Supplier shall work with the Authority's Service Integration team to ensure that the SOC is designed to capture data once, minimising the need for manual data capture and input.

43.3 Service Integration (SI) Tools

Ref	Level	Owner	Description
43.3.1	L3	Supplier	The Supplier shall fully integrate with or use the ITSM Product at its own cost. Where the Supplier provides, manages, operates and maintains its own service management tools and interfaces to the Authority's toolset, the Supplier shall bear all the responsibility and costs of creating, maintaining and operating such interface.
43.3.2	L3	Supplier	Where the Supplier provides its own service management products, then, in accordance with the Authority's Service Management Policies and Processes, the Supplier shall: a) set-up, operate and maintain those tools and interfaces to integrate with the Authority's product; b) identify and resolve Defects and performance failures in its service management products, interfaces and processes; and c) exchange data with the Authority, in the format agreed with the Authority, and in line with the Authority's Policies and Processes.
43.3.3	L3	Supplier	The Supplier shall identify any issues and recommend action to address any issues identified in the SIEM Toolset, Supplier's ITSM Product, interfaces and processes to the Authority.

43.4 Data

Ref	Level	Owner	Description
43.4.1	L3	Supplier	The Supplier shall ensure that the Authority is provided with SOC data in a timely manner and which is accurate to format and content agreed by the Authority.
43.4.2	L3	Supplier	The Supplier shall ensure all Authority Data created, stored or modified by the Supplier in the delivery of the Services remains materially accurate, up to date and in line with the Authority's Policies and Processes and Schedule 11 (<i>Processing of Personal Data</i>).
43.4.3	L3	Supplier	The Supplier shall ensure that all system information and log information is retained for a period of 12 months and made available to the Authority when requested or notified as a Security Incident. The Authority may ask the Supplier to retain these reports for a longer period of time (i.e. in the event where there is an active investigation under way).
43.4.4	L3	Supplier	The Supplier shall raise an Information Security Incident after it becomes aware of an event that impacts the confidentiality, integrity or availability of the service, such as a loss of service or Breach of Security.

43.5 Location and Disaster Recovery

Ref	Level	Owner	Description
43.5.1	L3	Supplier	The Supplier shall be located and operate all the SOC services from within the boundaries of the United Kingdom.
43.5.2	L3	Supplier	The SOC shall be operated at Supplier Premises; such premises are to be in-line with the Authority's requirements for processing of data.
43.5.3	L3	Supplier	The Supplier shall deliver all of its services from premises that meet the relevant requirements of ISO27001 and Cyber Essentials Plus and promote appropriate levels of joint working with the Authority and Other Suppliers.

43.5.4	L3	Supplier	The Supplier shall ensure there is a Service Continuity Plan in place for the SOC. This shall include the provision of adequately skilled Supplier resource with Authority specific knowledge.
43.5.5	L3	Supplier	The Supplier shall ensure that the Service Continuity Plan is tested at least annually; and put in place remediation, if required, of failure findings arising from the annual testing.
43.5.6	L3	Supplier	The Supplier shall ensure that the Authority has access to the Service Continuity Plan and the SOC service continuity is in line with the Authority's IT Service Continuity Management Policies and Processes.
43.5.7	L3	Supplier	The Supplier will obtain the Authority's approval for changes to the tools and processes used to provide for online reporting or enquiry facilities.

43.6 Security Management Function Performance

Ref	Level	Owner	Description
43.6.1	L3	Supplier	The Supplier shall develop and maintain security systems and processes to enable a service that meets the Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>).
43.6.2	L3	Supplier	The Supplier shall work to improve process and tooling, automation and simplification with the Authority and other parties to enable a culture of Continual Service Improvement and innovation to constantly improve Authority experience in line with the Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>).

43.7 Security Workshops

Ref	Level	Owner	Description
43.7.1	L3	Supplier	The Supplier shall provide appropriately skilled and experienced personnel to attend workshops and meetings concerning security whenever reasonably requested by the Authority.
43.7.2	L3	Supplier	The Supplier shall provide to the Authority such input concerning the Services as the Authority may reasonably require, to assist it in producing meaningful, timely and accurate reports for security meetings and workshops.
43.7.3	L3	Supplier	The Supplier shall provide security advice and technical support as reasonably requested by the Authority from time to time.

43.8 Business Continuity and Disaster Recovery Planning

Ref	Level	Owner	Description
43.8.1	L3	Supplier	The Supplier shall assist with business continuity and disaster recovery processes in the event of a Breach of Security for the Services in line with the ITSCM Policies and Processes.

43.9 Security Mailbox Management

Ref	Level	Owner	Description
43.9.1	L3	Supplier	The Supplier shall provide a SOC mailbox and undertake responses to all queries and such activities as required. The Supplier will respond to urgent escalations within one (1) hour and to routine enquiries within twenty-four (24) hours.

43.10 Reporting

Ref	Level	Owner	Description
43.10.1	L3	Supplier	The Supplier shall provide the Authority with a monthly Management Information report based on agreed Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>).
43.10.2	L3	Supplier	The Supplier shall meet the Authority's changing operational Management Information reporting and dashboarding requirements in accordance with the Authority's Change Management Policies and Processes.
43.10.3	L3	Supplier	The Supplier shall provide metrics against each of the security service obligations that fully demonstrate the quality and timeliness of the delivery of the respective security Service.
43.10.4	L3	Supplier	The Supplier shall promptly provide the Authority, in the format required by the Authority, with information relating to the Security Operations Centre as may be requested from time to time.
43.10.5	L3	Supplier	The Supplier shall deal with any areas of improvement relating to the SOC in accordance with the CSI Management Policies and Processes.
43.10.6	L3	Supplier	The Supplier shall provide the Authority with access to real-time, and drillable, reporting dashboards.
43.10.7	L3	Supplier	The Supplier shall provide reports to the Authority to include, but not be limited to the following: a. number of malware Incidents; b. number of phishing attacks and Incidents; c. total number of Events; d. number of failed phishing attempts; e. number of false/positives; f. Policy violations; and g. number of authentication errors.

43.11 Development and promulgation

Ref	Level	Owner	Description
43.11.1	L3	Supplier	The Supplier shall input to the Authority its recommendations for updates and assist the Authority to maintain and keep current the SOC service descriptions and other related documents.
43.11.2	L3	Supplier	The Supplier shall inform the Other Suppliers of any Changes to the services relating to the Security Operations Centre (which includes the security Policies, the security standards, the security processes and other related documents).

44. SOC Strategy, Governance, Compliance and Risk Management

44.1 Service Integration (SI) Processes

Ref	Level	Owner	Description
44.1.1	L3	Supplier	The Supplier must be able to demonstrate compliance with Cyber Essentials, Cyber Essentials Plus, ISO/IEC 20000-1:2018, ISO/IEC 27001:2017, and ISO/IEC 23001-14:2019 (or successor standards).
44.1.2	L3	Supplier	The Supplier shall design and implement cross functional service management process interfaces in accordance with the standards and designs specified in the Authority's Service Management Policies and Processes. Such process designs and implementations shall include documented Operating Procedures that comply with the Authority's Service Management Policies and Processes.
44.1.3	L3	Supplier	The Supplier shall update the ITSM Product with service management data, templates, process documentation and reports used in the delivery of the Services.
44.1.4	L3	Supplier	The Supplier shall report immediately any Breach of Security to the Authority's Head of Security Operations in accordance with the Authority's Information Security Policy and Standards.

44.2 Supplier Service Description, Policy and Process Reviews

Ref	Level	Owner	Description
44.2.1	L3	Supplier	The Supplier shall provide the Authority with recommendations for updates and assist the Authority in maintaining and keeping current the SOC service descriptions and other related documents that may be produced.
44.2.2	L3	Supplier	The Supplier shall continually review the services relating to the Security Operations Centre and the Authority's Information Security Policy and Standards and make recommendations to the Authority on how such Services can be improved.
44.2.3	L3	Supplier	In reviewing the SOC related documents the Supplier shall take into account any input received from the Authority in relation to the Authority's Other Suppliers' review of those documents.

44.3 Changes and Amendments

Ref	Level	Owner	Description
44.3.1	L3	Supplier	The Supplier shall provide the Authority with a Security Impact and Risk Report as part of any addition or amendment to the Services.
44.3.2	L3	Supplier	The Supplier shall ensure that the Security Impact and Risk Report provided to the Authority by the Supplier takes into account and reflects all relevant Security Impact and Risk Reports received by the Supplier from the Authority's Other Suppliers via the Authority.
44.3.3	L4	Authority	The Authority shall inform the Supplier as soon as reasonably possible, following the receipt of any Security Impact and Risk Reports from Other Suppliers, whether it wishes the Supplier to proceed with the Changes to the Service

		Integration Services identified. In the event that the Authority wishes to proceed with the Changes identified, the Supplier shall process such Changes in accordance with the Authority's Change Management Policies and Process.
44.3.4	L3	Supplier The Supplier shall agree all Changes to Information Security Policies and Standards with the Authority before implementation or updates.

44.4 Security Service Improvements

Ref	Level	Owner	Description
44.4.1	L3	Supplier	The Supplier shall continually monitor the provision of the services relating to the Security Operations Centre, taking into account any changes in legislation, technology and standards, and make recommendations to the Authority from time to time as to how the security services and associated assurance Procedures could be improved. Following approval by the Authority, the Supplier shall process any proposed improvements in accordance with the Authority's Change Management Policies and Processes.
44.4.2	L3	Supplier	The Supplier shall perform, with the Authority's Security Team, a formal review of all security services, on a six-monthly basis, as agreed with the Authority, and subsequently the Supplier shall share the documented output with the Authority.
44.4.3	L3	Supplier	The Supplier shall regularly perform a formal review of all Processes, Procedures, guidance and instructions to confirm compliance with the Security Management Plan and the Information Security Policy and Standards, as a minimum, on an annual basis (12-month intervals).
44.4.4	L3	Supplier	Where the Supplier identifies an improvement to the security services, the Supplier shall provide reports of all findings and recommendations to the Authority, which shall include activities, impact and timescales for any improvements identified. The Supplier shall agree implementation timescales for these improvements with the Authority.
44.4.5	L3	Supplier	Once the activities and timescales in the security services improvement report have been agreed with the Authority, the Supplier shall create, maintain and update a consolidated plan detailing such agreed activities, and the timescales for completing such activities including any costs which shall be agreed with the Authority, covering each security Service (" Security Services Improvement Plan "). The Supplier shall implement the activities set out in the Security Services Improvement Plan in accordance with the agreed timescales therein.

44.5 Security Alerts and Notices

Ref	Level	Owner	Description
44.5.1	L3	Supplier	In line with the Authority's timescales, the Supplier shall review the relevance and impact of all security alerts and notices of threats, risks and vulnerabilities applicable to the Services and revert to the Authority with details of the same.
44.5.2	L3	Supplier	The Supplier shall provide progress reports to the Authority in accordance with the timescales requested by the Authority and the Performance Indicators and Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>) (having due regard to the potential severity of the Information Security Event).
44.5.3	L3	Supplier	The Supplier shall ensure it is the central point for receipt of any security alerts, briefings, technical notices or communications, for the Services.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

44.5.4	L3	Supplier	The Supplier shall ensure that any information received from the Authority or any of the Authority's Other Suppliers, in response to a security alert or notice issued by it, is addressed in the appropriate manner.
--------	----	----------	---

45. Security Protect, Control, Maintain and Train

45.1 Access and Prohibited System Usage

Ref	Level	Owner	Description
45.1.1	L3	Supplier	The Supplier shall provide the Authority with such information and assistance as the Authority may reasonably require, in complying with the Supplier's obligation to continuously monitor the use of the services by Supplier Personnel and the Authority Personnel.
45.1.2	L3	Supplier	The Supplier shall provide the Authority with such access to any device and data controlled by the Supplier, in relation to the services provided, as may be reasonably requested by the Authority from time to time.
45.1.3	L3	Supplier	The Supplier shall ensure that the SOC can block access based on geo location with exemptions being granted by the Authority's Security Team.
45.1.4	L3	Supplier	If requested by the Authority, the Supplier shall conduct investigations into unauthorised access on behalf of the Authority and provide the findings to the Authority.

45.2 Internet access service

Ref	Level	Owner	Description
45.2.1	L3	Supplier	The Supplier shall carry out regular reviews and recommend updates to the "blacklist" and the "whitelist". The Supplier shall carry out such reviews on a monthly basis.
45.2.2	L3	Supplier	The Supplier shall manage "whitelist" activity in accordance with the Authority's Request Fulfilment Policy and Process.

45.3 Audit Trails

Ref	Level	Owner	Description
45.3.1	L3	Supplier	The Supplier shall, whenever requested by the Service Integration function or directly by the Authority, provide the Authority's Other Suppliers with information concerning the Processes required to be followed by the Other Suppliers in order to generate any audit trails required to be produced pursuant to the Services, including but not limited to, non-compliances, Incidents and Events.
45.3.2	L3	Supplier	The Supplier shall identify, document and review each audit trail produced by it in accordance with the Authority's Information Security Policy and Standards and the Security Management Plan. The Supplier shall then notify the Authority of any unusual or anomalous activity in such audit trails along with any such activity notified to it by the Authority's Other Suppliers. The Supplier shall also review audit trails will need to be reviewed in accordance with the timeframes defined by the Authority.

46. Security Information and Event Management (SIEM)

46.1 Security Information and Event Management (SIEM)

Ref	Level	Owner	Description
46.1.1	L3	Supplier	The Supplier shall provide the Authority with a SIEM Service, pursuant to which the Supplier shall consolidate and analyse the logs of devices and appliances agreed with the Authority which are installed across the Other Suppliers and observe Authority Data activity both inside and outside the Authority's network perimeter which could expose the infrastructure provided across the Other Suppliers to a Security Risk. The Supplier shall in respect of any Security Risk identified instigate remedial action as is required.
46.1.2	L3	Supplier	The Supplier shall configure the content management element of the SIEM solution and provide the Authority with details of this configuration and details of subsequent changes to the configuration.
46.1.3	L3	Supplier	The Supplier shall comply with and provide evidence (when reasonably requested by the Authority) of the Supplier's compliance with industry and government best practice, for example the NCSC standards.
46.1.4	L3	Supplier	The Supplier shall ensure that the SIEM service collects logs and relevant data or information from any item of equipment or Authority's service provision, including, End User Client Devices, network devices, servers, application security logs, anti-virus, proxy server, access control system, security solutions, TLS VPN Gateway, WAF, VA Tool, Anti-phishing and Anti-malware.
46.1.5	L3	Supplier	The Supplier shall deliver Updates, patches, bug fixes and version Upgrades to the SIEM Service. The Supplier shall maintain all patches, Updates and bug fixes to current or N-1.
46.1.6	L3	Supplier	The Supplier shall ensure that the SIEM solution meets the required availability levels.
46.1.7	L3	Supplier	The Supplier shall ensure the SIEM service is integrated into the ITSM Product.

46.2 Implementation

Ref	Level	Owner	Description
46.2.1	L3	Supplier	The Supplier shall implement correlation rules based on out-of-box functionality and use cases of the SIEM solution. The Supplier shall inform the Authority of the alerting and reporting rules used for all standard logs.
46.2.2	L3	Supplier	The Supplier shall provide the SIEM Process and undertake development of the associated use cases and provide the impact of integrating new suppliers, businesses, rolling out new products and/or re-architecting the Authority's services.
46.2.3	L3	Supplier	The Supplier shall provide the capability for the Authority to view and monitor the progress of Alerts in real-time or near real-time.
46.2.4	L3	Supplier	The Supplier shall provide configurable Incident Management dashboard/reports for the Authority, from its system via a secure web interface, and shall modify the same as per the changing requirements of the Authority.

46.3 Information Security Events

Ref	Level	Owner	Description
46.3.1	L3	Supplier	When aware of an Information Security Event, as soon as possible or in accordance with any relevant Performance Indicators and Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>) (having due regard to the potential severity of the Information Security Event), the Supplier shall inform the Authority of that Information Security Event.
46.3.2	L3	Supplier	Following the categorisation of any Information Security Event as an Information Security Incident, the Supplier shall inform the Authority of that Information Security Incident in accordance with Authority's Service Management Policies and Processes.

46.4 Intrusion Detection and Prevention Systems (IDPS)

Ref	Level	Owner	Description
46.4.1	L3	Supplier	The Supplier shall review and manage the IDPS Events and rules and raise Security Incidents in accordance with the Authority's Incident Management Policies and Process.

46.5 Advanced Malware Protection (AMP)

Ref	Level	Owner	Description
46.5.1	L3	Supplier	The Supplier shall review and manage AMP Events and activity and raise Security Incidents in accordance with the Authority's Incident Management Policies and Process.

46.6 Mitigate Advanced Persistent Threat (APT)

Ref	Level	Owner	Description
46.6.1	L3	Supplier	The Supplier shall monitor the IT Environment for Advanced Persistent Threats and suggest appropriate action to the Authority on an on-going basis in accordance with the Technical Framework Document.

46.7 Anti-Virus / Malware Analysis

Ref	Level	Owner	Description
46.7.1	L3	Supplier	The Supplier shall review all the anti-virus/malware Alert messages, manage them accordingly and promptly make the information available to the Authority.
46.7.2	L3	Supplier	The Supplier shall review all the anti-virus/malware coverage within the scope of its services and manage in accordance with the Authority's Policies and Processes.
46.7.3	L3	Supplier	The Supplier shall analyse any malware to ascertain its severity impact and assign a risk level.

46.8 Anti-Phishing, Anti-Malware, Protective Threat (PT)

Ref	Level	Owner	Description
46.8.1	L3	Supplier	The Supplier shall provide the Authority with a real-time dashboard view of the risks/threats identified through the anti-phishing and threat intelligence Services.
46.8.2	L3	Supplier	The Supplier shall provide to the Authority appropriate reports in regard to the risks/threats identified through the anti-phishing and threat intelligence Services.

46.9 Event / Incident Identification

Ref	Level	Owner	Description
46.9.1	L3	Supplier	The Supplier shall perform the agreed monitoring and advise on remediation of Events in accordance with the Authority's Policies and Processes, the Performance Indicators and the Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>).
46.9.2	L3	Supplier	The Supplier shall provide input regarding the Services to the Authority's retained Service Integration function's Incident response Process and toolset, including priority definitions for security related Incidents.

46.10 Firewall Governance and Compliance

Ref	Level	Owner	Description
46.10.1	L3	Supplier	The Supplier shall perform continuous Firewall monitoring in accordance with the Authority's requirements.
46.10.2	L3	Supplier	The Supplier shall recommend to the Authority any remediation activity highlighted by the Supplier's ongoing monitoring and assessments Firewalls.

46.11 Content and Context Analytics

Ref	Level	Owner	Description
46.11.1	L3	Supplier	The Supplier shall analyse the contents of relevant Authority Data and the way in which it is being used in order to detect any violations of the Authority's Information Security Management Policies and Standards.

47. Security Incident Response

47.1 Proactive Response

Ref	Level	Owner	Description
47.1.1	L3	Supplier	The Supplier shall proactively manage current and emerging threats and report and raise Security Incidents in accordance with the Authority's Incident Management Policies and Processes.

47.2 Forensic Readiness Policy and Plans

Ref	Level	Owner	Description
47.2.1	L3	Supplier	The Supplier shall provide specialist forensic investigation support when requested by the Authority.
47.2.2	L3	Supplier	The Supplier shall develop a forensic readiness plan, with input, review and approval from the Authority, that sets out tasks and Procedures that can be put in place before a Security Incident occurs to ensure that the Authority is best placed to deal with the demands placed upon it when a Security Incident involving electronic Authority Data occurs.
47.2.3	L3	Supplier	The Supplier shall work proactively with the Authority to develop an agreed Process to respond to requests for forensic investigation, in accordance with the Authority's Change Management Policies and Processes. The Supplier shall develop such Processes as catalogue items.
47.2.4	L3	Supplier	The Supplier shall ensure that Supplier Personnel undertaking forensic activity are suitably trained and where necessary appropriately qualified in digital forensics and Incident Management.
47.2.5	L3	Supplier	The Supplier shall provide forensic analysis within the agreed and authorised scope of work and in compliance with current government and legal standards and requirements.

47.3 Forensic Investigation

Ref	Level	Owner	Description
47.3.1	L3	Supplier	The Supplier shall, at the request of the Authority and using the agreed Process, provide personnel who are appropriately trained and experienced to use forensic tools and tested methods to support the Authority investigations and Incidents. Where the Supplier utilises third parties, or resources unfamiliar with the operation of the Authority's forensic processes, the Supplier shall be responsible for all Authority Data and reports submitted to the Authority and will undertake a full peer review prior to submission to ensure accuracy of information in accordance with Authority Standards, Policies and Procedures.
47.3.2	L3	Supplier	The Supplier shall, at the request of the Authority, capture data related to an authorised investigation request of Authority Data, including desktop PCs, laptops, server shares, mobile phone or other storage media currently present or in the future.
47.3.3	L3	Supplier	Where authorised by the Authority to do so, the Supplier shall provide forensic analysis of captured Authority Data to support ongoing investigations and Security Incident responses and present reports supporting the findings of the analysis in accordance with the agreed forensic methodology and Process.

47.4 Incident Response Improvements

Ref	Level	Owner	Description
47.4.1	L3	Supplier	The Supplier shall incorporate Lessons Learnt from execution of Incident response playbooks and their outcomes – where the Supplier encounters new and unplanned Incidents, the Supplier will ensure that new use cases and playbooks are created and Tested.
47.4.2	L3	Supplier	The Supplier shall, on a monthly basis, review the response activities to Security Incidents and ensure that all Lessons Learnt are incorporated into future detection and response activities
47.4.3	L3	Supplier	The Supplier will revise overall response strategies as required based on the monthly analysis of Incidents encountered.

48. Recovery Service

48.1 Recovery plans and strategy Improvements

Ref	Level	Owner	Description
48.1.1	L3	Supplier	The Supplier shall incorporate Lessons Learnt from execution of Incident recovery playbooks and their outcomes – where the Supplier encounters new and unplanned Incidents. the Supplier will ensure that new use cases and playbooks are created and Tested.
48.1.2	L3	Supplier	The Supplier shall, on a monthly basis, review the recovery activities to Security Incidents and ensure that all Lessons Learnt are incorporated into future recovery activities.
48.1.3	L3	Supplier	The Supplier will revise overall recovery strategies as required based on the monthly analysis of Incidents encountered.

Network Operations Services Descriptions

49. Network Operations Centre Services

49.1 Introduction

Ref	Level	Owner	Description
49.1.1	L3	Supplier	The Supplier shall ensure that the Network Operations Centre operates as an integral part of the Supplier's Service Integration function.
49.1.2	L3	Supplier	The Supplier shall ensure that the Network Operations Centre operates 24hrs a day, 365 days a year, and serves those sites and services as identified in the Technical Framework Document.
49.1.3	L3	Supplier	The Supplier shall use the ITSM Product in the management and execution of its activities in concert with the use of and adherence to the Authority's Service Management Processes aligned to ITIL v4.

49.2 General

Ref	Level	Owner	Description
49.2.1	L3	Supplier	The Supplier shall respond to the current and future requirements of the Authority, by proactively anticipating needs, and adjusting services accordingly, and wherever possible, containing costs within the agreed Charges. Requirements for new services and any proposed changes to the agreed Charges will be handled through the Authority's Change Management Policy and Process and the Change Control Procedure set out in Schedule 8.2 (<i>Change Control Procedure</i>) and the Supplier will work with the Authority to assess the impact of any Changes to the operational of the Authority's wider IT services and budgets.
49.2.2	L3	Supplier	The Supplier shall work with the Authority to establish, maintain and enhance NOC Processes, governance and tools that support the Supplier's end to end responsibility and enable it to provide consistent management, coordination and communication of the delivery of the NOC services across the supply chain.
49.2.3	L3	Supplier	To allow for the inclusion of Other Suppliers and/or Resolver Groups to benefit from the NOC services in the future, the Supplier shall ensure any supporting processes and technology employed by the Supplier, in addition to the Authority's process and chosen ITSM Product, are scalable and adaptable to allow for the inclusion of Other Suppliers and potential increases/decreases to volumes.
49.2.4	L3	Supplier	The Supplier shall comply with all Authority Policies and Processes.
49.2.5	L3	Supplier	The Supplier shall maintain appropriate documents and records in connection with the provision of the Network Operations Centre services and shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the Supplier's compliance with all applicable Policies, Processes, Procedures and service obligations.
49.2.6	L3	Supplier	The Supplier will co-operate with and promote joint working between the Supplier, the Authority, and the Other Suppliers where activities require a multi-party approach.
49.2.7	L3	Supplier	The Supplier shall work within a governance timetable, defined by the Authority, of regular events for recurring activities and shall also act on agreed triggers for event driven activities.
49.2.8	L3	Supplier	The Supplier will participate in, and chair, regular meetings, at least once per Quarter, with Other Suppliers to identify, analyse and give recommendations for Continual Service Improvement opportunities.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

49.2.9	L3	Supplier	The Supplier shall support the information exchange between and among the Other Suppliers and the Authority as directed by the Authority and work with the Authority to drive Continual Service Improvement and improvement of the Service Management Processes.
49.2.10	L3	Supplier	The Supplier shall establish and manage controls to ensure that its Processes and interfaces are auditable and meet all the regulatory and policy requirements set out in this Agreement.
49.2.11	L3	Supplier	To promote process efficiency and data quality, the Supplier shall ensure the Network Operations Centre Processes are automated wherever possible. The Supplier shall ensure that the Network Operations Centre is designed to capture data once, minimising the need for manual data capture and input. The Supplier shall ensure all data is, wherever possible, validated by the ITSM Product on input.
49.2.12	L3	Supplier	The Supplier shall assist the Authority to identify automation opportunities, develop tools/scripts and enhancing Processes (including assisting with integrations to other third party toolsets where required), to proactively perform and automate the Service Management Processes and implement any tools/scripts to support the Service Management Process in accordance with the Authority's Change Management Policies and Processes and Schedule 8.2 (<i>Change Control Procedure</i>), as applicable.

49.3 Location and Disaster Recovery

Ref	Level	Owner	Description
49.3.1	L3	Supplier	The Supplier shall be located and operate all NOC services from within the boundaries of the United Kingdom.
49.3.2	L3	Supplier	The NOC shall be operated at Supplier Premises; such premises are to be in-line with the Authority's requirements for processing of data including in accordance with Schedule 11 (<i>Processing of Personal Data</i>).
49.3.3	L3	Supplier	The Supplier shall deliver all of its services from premises that meet the relevant requirements of ISO27001 and Cyber Essentials Plus and promote appropriate levels of joint working with the Authority and Other Suppliers.
49.3.4	L3	Supplier	The Supplier shall ensure there is a Service Continuity Plan in place for the NOC. This shall include the provision of adequately skilled Supplier resource with Authority specific knowledge.
49.3.5	L3	Supplier	The Supplier shall ensure that the Service Continuity Plan is tested at least annually; and put in place remediation, if required, of failure findings arising from the annual testing.
49.3.6	L3	Supplier	The Supplier shall ensure there is a Service Continuity Plan in place for the Network Operations Centre and that it is tested at least annually. The Supplier shall put in place remediation if required and as approved by the Authority.
49.3.7	L3	Supplier	The Supplier will obtain the Authority's approval for changes to the tools and processes used to provide for online reporting or enquiry facilities.

49.4 Network Operation Centre Activity

Ref	Level	Owner	Description
49.4.1	L3	Supplier	The Supplier shall provide network operations services managing all network devices, including: a) monitoring and analysis b) troubleshooting and remote resolution of physical issues such as power supplies and cable connections c) troubleshooting and remote resolution of logical issues such as routing and Firewall misconfigurations

			d) network Incident escalation and reporting, e) network break-fix actions.
49.4.2	L3	Supplier	The Supplier shall continuously monitor the ITSM Product and Other Tooling for new or escalated Alerts and Service Tickets.
49.4.3	L3	Supplier	The Supplier shall notify the Major Incident Management team, via e-mail and/or telephone as directed in standard Operating Procedures, of any Major Incidents and outages affecting the Authority's network. The Supplier shall update progress and status regularly, as outlined in the standard Operating Procedures.
49.4.4	L3	Supplier	The Supplier shall follow documented triage Procedures in order to identify if a Major Incident is related to physical or logical issues.
49.4.5	L3	Supplier	The Supplier shall troubleshoot issues including: a) isolation and resolution of power and physical connection issues; b) isolation and resolution of routing, Firewall, and device misconfigurations; c) isolation and resolution of failing or compromised network redundancy; d) isolation and resolution of network security vulnerabilities and Incidents; e) network performance and availability; and f) data and deep packet analysis.
49.4.6	L3	Supplier	The Supplier shall use the Authority's approved documented Procedures when engaging external support organisations such as on-site support or vendor support to assist or facilitate resolution of network Incidents.
49.4.7	L3	Supplier	The Supplier shall notify the Authority when engagement with external support organisations do not meet expectations.
49.4.8	L3	Supplier	When break-fix actions (configuration changes required to restore operation or connectivity to a device or service) are required, the Supplier shall perform break-fix actions in accordance with all documented Authority Policies and Standards.
49.4.9	L3	Supplier	When the Authority's on-site support teams are installing new devices or replacing existing devices, the Supplier shall provide telephone support to verify connectivity of the affected devices and validate the appropriate configuration of the devices.

49.5 Alert Management

Ref	Level	Owner	Description
49.5.1	L3	Supplier	The Supplier shall proactively monitor the Network Services to detect faults, monitor the availability of the Network Services and detect if performance thresholds (including the Target Performance Levels) have not been met.
49.5.2	L3	Supplier	The Supplier shall provide Alerts via an electronic interface into the Supplier Systems to a specification agreed between the Supplier and the Authority.

49.6 Performance and Availability Management

Ref	Level	Owner	Description
49.6.1	L3	Supplier	The Supplier shall perform Availability Management in accordance with the Availability Management Processes, Policies and Procedures.
49.6.2	L3	Supplier	The Supplier shall collate information concerning the availability elements in accordance with the relevant interface and integration requirements.
49.6.3	L3	Supplier	The Supplier shall identify availability elements of the Services using support from the Authority in identifying the key availability elements where required.
49.6.4	L3	Supplier	The Supplier shall develop the Availability Plan in accordance with the Availability Management Processes, Policies and Procedures. The Supplier shall ensure the Availability Plan ensures that all services are appropriately monitored with suitable Event and Alert regimes in place to identify any degradation in service.
49.6.5	L3	Supplier	The Supplier shall conduct a network trend analysis to compile daily and long-term reports for various network traffic areas of interest, as requested by the Authority. The Supplier shall ensure that such reports supply both generalised and specific information about targeted areas and provide useful snapshots of information. In addition, the Supplier shall ensure such reports include daily and weekly reports covering various error conditions, workload (i.e. CPU and memory), and network utilisation. The Supplier shall also provide customised trend analysis reports based on current monitoring capabilities.
49.6.6	L3	Supplier	The Supplier shall perform data collection using monitoring tools approved by the Authority, for input to network capacity planning when triggered by a Network Availability Event.
49.6.7	L3	Supplier	The Supplier shall determine bandwidth utilisation using network and configuration information against predetermined Network Availability thresholds.
49.6.8	L3	Supplier	The Supplier shall make recommendations to the Authority based on monitoring, reporting and analysis of site data and configurations to improve overall site resilience, availability, bandwidth, utilisation and performance.
49.6.9	L3	Supplier	The Supplier must use information to better estimate future requirements based on application, organisational, or technology changes as well as adjustments to provide improved cost/benefit resources.
49.6.10	L3	Supplier	The Supplier shall provide continuous Network Availability monitoring using software provided or approved by the Authority.
49.6.11	L3	Supplier	The Supplier shall conduct verification and validation of Network Availability of outage statistics and monitor the Authority network Quality of Service (QoS) to ensure services are adequate for specific applications and that these services continue to meet the Authority's requirements.
49.6.12	L3	Supplier	The Supplier shall provide continuous administration, account management, and asset management for tools utilised by Network Operations.

50. LAN Services

50.1 Introduction

Ref	Level	Owner	Description
50.1.1	L3	Supplier	The Supplier shall provide all aspects of the provision and ongoing management of the local area networks on Sites as documented in the Technical Framework Document.
50.1.2	L3	Supplier	The Supplier shall manage all aspects of security, performance, availability and resilience to ensure High Availability (HA) in accordance with the Target Performance Levels set out in Schedule 2.2 (<i>Performance Levels</i>).
50.1.3	L3	Supplier	The Supplier shall comply with https://www.gov.uk/guidance/how-to-install-network-infrastructure-in-shared-buildings (particularly, but not restricted to, the section on Local Area Networks) including any updates to such standards during the Term.

50.2 LAN Active Port Services

Ref	Level	Owner	Description
50.2.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide switched and non-switched connections as required to workstations, Print Devices, and other shared network resource End User Client Devices within each Site.
50.2.2	L3	Supplier	The Supplier shall provide fly-leads for switched and non-switched connections, where not present.
50.2.3	L3	Supplier	At each Site on each occasion that LAN Port installation is undertaken by the Supplier at the request of the Authority, the Supplier shall, without prejudice to any other obligation of the Supplier, utilise existing cabling where practicable for the purpose of such LAN Port installation. If any existing cabling (installed by the Supplier) that it should have been possible to utilise is not damaged, but is inadequate, the Supplier shall make good such cabling at no additional charge to the Authority.
50.2.4	L3	Supplier	The Supplier shall monitor the reliability of all Site LAN cabling at Authority Premises and recommend an investigation to the Authority (at additional cost) if the level of Site LAN cable faults is excessive in the reasonable opinion of the Supplier. When making such recommendation, the Supplier shall provide to the Authority evidence of the rate of Site LAN cable faults occurring at the affected Site(s). The Supplier shall undertake such investigation if requested by the Authority as a Project.
50.2.5	L3	Supplier	The Supplier shall report to the Authority on the number of LAN cable faults on a per Site basis per Service Period.
50.2.6	L3	Supplier	The Supplier shall provide the active port service at Authority Premises to include the following levels of traffic prioritisation to enable different performance characteristics to be applied to the Authority's traffic: a) Class 1 – real-time voice traffic; b) Class 2 – video and business critical data application traffic with up to four sub levels but a minimum of three sub levels (class 2a, class 2b and class 2c) to provide for differentiated performance levels; c) Class 3 – including non-business critical data application traffic.
50.2.7	L3	Supplier	The Supplier shall utilise industry standard traffic classification and delineation techniques to provide the traffic prioritisation for the active port service to meet the business critical data requirements of the Authority, as modified from time to time, at Transformed Sites.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

50.2.8	L3	Supplier	The Supplier shall ensure that Authority Premises have sufficient flexibility to enable the Service to be enhanced as required in the future
50.2.9	L3	Supplier	For all Sites, the Supplier shall provide the active port services up to and including the following Service end points: a) Where there is the Authority equipment, the interface cable between each item of the Authority equipment and the wall, floor or IP telephone socket, as the case may be; b) Where there is an IP telephone from which there is no connection to the Authority equipment, the LAN Port on that IP telephone; and c) Where there is a wireless LAN device, the wireless Access Point.
50.2.10	L3	Supplier	The Supplier shall monitor usage of the active port services including Site LAN switch port traffic statistics and other similar measures to identify Inactive Ports.
50.2.11	L3	Supplier	The Supplier shall report to the Authority each Service Period, all Inactive Ports at each Site during the Service Period immediately prior to the report. In such report the Supplier shall identify, in respect of each such Inactive Port, the Services which the Authority is paying the Supplier to be provided through or using that Inactive Port.
50.2.12	L3	Supplier	The Supplier shall cease provision of each Inactive Port (together with all Services provided by the Supplier through or using that Inactive Port) as requested by the Authority in accordance with the Service Request Procedure. Services which the Supplier ceases to provide in accordance with this Paragraph 50.2.11, shall be in relation only to the Inactive Ports which the Supplier ceases to provide, and not any active ports.

50.3 Wireless LAN Scope

Ref	Level	Owner	Description
50.3.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide wireless LAN (WLAN) connections to all workstations, Print Devices, and other shared network resource end devices identified as in scope of the Wireless network and in the Authority Premises as identified in the Authority's Technical Framework Document.
50.3.2	L3	Supplier	The Supplier shall comply with https://www.gov.uk/guidance/how-to-install-network-infrastructure-in-shared-buildings (particularly, but not restricted to, the section on wireless Networks) including any updates to such standards during the Term.
50.3.3	L3	Supplier	The Supplier shall provide End User authentication facilities accredited to be in compliance with the Authority's Security Policies, as amended from time-to-time.
50.3.4	L3	Supplier	The Supplier shall provide encryption facilities accredited to be in compliance with the Authority's Security Policies and Schedule 2.4 (<i>Security Management</i>), as amended from time-to-time.
50.3.5	L3	Supplier	The Supplier shall monitor and manage the building coverage and available wireless bandwidth for End Users during core Service Hours and ensure that End Users do not experience any performance degradation attributed to the Network.

50.4 VLAN Scope

Ref	Level	Owner	Description
50.4.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide Virtual LAN (VLAN) configurations to support LAN management and partitioning as required.
50.4.2	L3	Supplier	The Supplier shall modify VLAN provision with insertions and modifications to configuration to support Changes in the Authority Requirements from time-to-time.

51. Wide Area Network (WAN) Services

51.1 Introduction

Ref	Level	Owner	Description
51.1.1	L3	Supplier	The Supplier shall work with the existing MPLS WAN supplier and the Existing Supplier as needed. The Existing Supplier will continue to manage the delivery and service management activity related to the MPLS WAN service up until the point this service is removed, at the end of the Existing Supplier Contract. The Supplier shall ensure that all service descriptions in paragraph 51 are services that are not dependant on the legacy MPLS WAN infrastructure.
51.1.2	L3	Supplier	The Supplier shall comply with https://www.gov.uk/guidance/how-to-install-network-infrastructure-in-shared-buildings (particularly, but not restricted to, the section on WAN) including any updates to such standards throughout the Term.
51.1.3	L3	Supplier	The Supplier shall ensure that where the Services are Public Services Network (PSN) services they will comply with relevant PSN standards and processes, as described on the PSN website: https://www.gov.uk/government/groups/public-services-network ("PSN Standards").
51.1.4	L3	Supplier	Where the Services are Health and Social Care Network (HSCN) connectivity services, the Supplier shall comply with the HSCN obligations and processes described in the following documents on the HSCN website: https://www.digital.nhs.uk/health-social-care-network/connectivity-suppliers : a) HSCN Compliance Operating Model; b) HSCN Obligations Framework; c) HSCN CN-SP Service Management Requirement Addendum; d) CN-SP Deed; and e) HSCN Mandatory Supplemental Terms.
51.1.5	L3	Supplier	The Supplier shall provide all aspects of the provision and ongoing management of the WAN on Authority Premises as documented in the Authority's Technical Framework Document.
51.1.6	L3	Supplier	The Supplier shall provide adequate management of all aspects of security, performance, availability and resilience to ensure availability in accordance with Schedule 2.2 (<i>Performance Levels</i>).
51.1.7	L3	Supplier	The Supplier shall plan, design, install, Test and provide all WAN and MAN equipment necessary to deliver the active bearer service.
51.1.8	L3	Supplier	The Supplier shall provide interconnection of the LAN services necessary to allow any LAN Port to access any other LAN Port or External Gateway Services.
51.1.9	L3	Supplier	The Supplier shall isolate the Authority traffic from any other Supplier customer traffic to ensure that the Authority's traffic is carried at a security level indicated in the security Policy and Standards.
51.1.10	L3	Supplier	The strategic direction of the Authority is that of a cloud-first, internet-first organisation, and the MPLS network links will be removed over time from all Sites and replaced with an Internet only solution. The Supplier shall work with the Authority and the Existing Supplier to ensure that any and all remaining dependencies on the MPLS are removed by the expiry/end of the Existing Supplier Contract, thus allowing for the removal of the MPLS circuits.

51.2 Remote Access Service

Ref	Level	Owner	Description
51.2.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide all infrastructure required to provide remote access services that enable End Users to access the Authority networks and systems via Internet-based connections. The scope of remote access is as specified in the Authority's Technical Framework Document.

51.3 Internet Access Service

Ref	Level	Owner	Description
51.3.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide all infrastructure required to provide an internet access service as described in the Technical Framework Document that: a) provides authenticated End Users secure access to the public internet; and b) allows authenticated or other agreed devices secure access to the public Internet. As per the Authority's Technical Framework Document.
51.3.2	L3	Supplier	The Supplier shall plan, design, install, Test and manage a Cloud Access Security Broker (CASB) and integrate it with the internet access service, as more particularly described in the Authority's Technical Framework Document.
51.3.3	L3	Supplier	The Supplier shall ensure that no End User is permitted access to the internet access service until that End User has been authenticated through the provision of a single sign-on using the Authority's approved authentication method, as at the Effective Date. Where such authentication cannot be established without further prompts, the Supplier shall provide an authentication method that uses username/password.
51.3.4	L3	Supplier	The Supplier shall ensure that the internet access service is provided in accordance with the Standards, as set out in Schedule 2.3 (Standards).
51.3.5	L3	Supplier	The Supplier shall manage End User access to internet sites using access controls in accordance with the Authority's guidelines and Policies pertaining to End User internet access as set out in Schedule 2.3 (Standards).
51.3.6	L4	Authority	The Authority shall procure Policies for group-based and individual access to the Internet to control Internet URL access and notify the Supplier of such Policies.
51.3.7	L3	Supplier	As required by the Authority and articulated in the Authority's Technical Framework Document, the Supplier shall implement the Authority's group-based policies to control access to certain Internet URLs which can be applied to different individuals or groups of individuals to provide flexible control of internet access, tailored to individual's and groups' business needs.
51.3.8	L3	Supplier	The Supplier shall perform filtering to block End User access to inappropriate URLs specified by the Authority and maintain a list of such inappropriate URLs, organised as a blacklist.
51.3.9	L3	Supplier	The Supplier shall perform filtering to block End User access to inappropriate categories of URLs specified by the Authority and maintain a list of such inappropriate categories of URLs, organised into blacklisted categories.
51.3.10	L3	Supplier	The Supplier shall perform, if required by the Authority, URL filtering to allow End User access only to appropriate URLs or categories of URLs, organised into White Listed Categories as an alternative to blacklisted categories.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

51.3.11	L3	Supplier	The Supplier shall ensure that on a 24-hour cycle, a daily information gathering process is undertaken to update the blacklisted categories and White Listed Categories as appropriate, to ensure that the lists of URLs within each category are accurate, complete and up to date.
51.3.12	L3	Supplier	The Supplier shall ensure that access to webpages containing words specified by the Authority are blocked for all End Users and include the URLs for such webpages in the blacklisted categories.
51.3.13	L3	Supplier	The Supplier shall ensure that access to webpages containing words specified by the Authority are allowed for all End Users and include the URLs for such webpages in the White Listed Categories.
51.3.14	L3	Supplier	The Supplier shall prioritise traffic across the Authority's network service to Internet addresses and services specified by the Authority as business-critical data, to ensure the performance of applications reliant on such traffic across the Authority's network service. By default, traffic to other Internet addresses and services shall not be prioritised as business-critical data.
51.3.15	L3	Supplier	The Supplier shall monitor all End User browser requests to detect viruses that have published virus signatures and block all such detected viruses from entering the active port service.
51.3.16	L3	Supplier	The Supplier shall apply all anti-virus signature releases automatically and apply all anti-virus software releases, as and when released by anti-virus vendors used by the Supplier.
51.3.17	L3	Supplier	The Supplier shall monitor all active content for inappropriate activity as agreed between the Parties and as amended from time to time. The Supplier shall ensure that it prevents any active content found to attempt to perform inappropriate activity from being executed.
51.3.18	L3	Supplier	The Supplier shall amend the access status of active content upon written request from the Authority's security group.
51.3.19	L3	Supplier	The Supplier shall log all End User browser requests, consolidate this data and archive it to non-re-writeable media. The Supplier shall make available to the Authority, at the Authority's request, such log data.
51.3.20	L3	Supplier	The Supplier shall retain the consolidated log data for a period of two years. At the end of this period, the Supplier shall dispose of such consolidated log data through a data disposal Procedure approved by the Authority (the Authority shall not unreasonably withhold or delay its approval to such a data disposal Procedure).
51.3.21	L3	Supplier	The Supplier shall provide Management Information systems that provide the Authority with End User internet patterns and profiles. Logs of such usage shall be kept by the Supplier for thirty (30) days, and reports made available to nominated End Users.

52. Voice Services

52.1 Voice Services

Ref	Level	Owner	Description
52.1.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide limited telephony infrastructure required to provide Voice Services as specified in the Authority's Technical Framework Document.

52.2 Softphone Client

Ref	Level	Owner	Description
52.2.1	L3	Supplier	The Supplier shall support and manage the configuration, integration and availability of the unified communications service using the solution specified in the Authority's Technical Framework Document.

52.3 Video Conference Service Scope

Ref	Level	Owner	Description
52.3.1	L3	Supplier	The Supplier shall plan, design, install, Test and provide all infrastructure required to provide for the delivery of a video conference service to the Authority as described in the Authority's Technical Framework Document.
52.3.2	L3	Supplier	The Supplier shall provide and manage the network infrastructure required to provide the video conference service with the video conference call capacity to meet the Authority's ongoing requirements.
52.3.3	L3	Supplier	The Supplier shall provide any Video Conference Endpoint equipment required by the Authority including, but not limited to, camera unit, monitor(s), trolley(s), and document imaging facilities, at any Site as nominated by the Authority.
52.3.4	L3	Supplier	The Supplier shall provide Video Conference Endpoint Configuration Management and hardware maintenance of the components required for the fixed Video Conference Endpoints and portable Video Conference Endpoints, at any Site as nominated by the Authority.
52.3.5	L3	Supplier	The Supplier shall provide an IP-based infrastructure to support the video conference service.
52.3.6	L3	Supplier	The Supplier shall provide the video conference service in compliance with the relevant international standards and/or proprietary standards in common industry use, as set out in Schedule 2.3 (<i>Standards</i>).
52.3.7	L3	Supplier	The Supplier shall enable video conferences to take place between any one Video Conference Endpoint or a group of the Authority Video Conference Endpoints and other compatible Authority or third party video conference facilities as described in the Technical Framework Document.
52.3.8	L3	Supplier	The Supplier shall provide clearly written instructions in non-technical language to assist video conference participants.
52.3.9	L3	Supplier	The Supplier shall establish multipoint video conference links between fixed Video Conference Endpoints and portable Video Conference Endpoints, or enable the Authority, if required by the Authority, to perform this function itself.

52.3.10	L3	Supplier	The Supplier shall enable the use of laptop-based desk-to-desk video conferencing. This shall provide, as a minimum, the following capabilities: a) enable point-to-point and multipoint desktop video conferences; b) provide interoperability with the existing fixed Video Conference Endpoints and portable Video Conference Endpoints; c) provide the ability to move between audio-only and full video conferencing; and d) enable End Users to participate in video conferences via the remote access service.
---------	----	----------	--

52.4 Contact Centre Service

Ref	Level	Owner	Description
52.4.1	L3	Supplier	The Supplier shall plan, design, install and provide all equipment necessary for the support of the Authority contact centre services as defined in the Authority's Technical Framework Document.

53. Network Infrastructure Services

53.1 Provision of a Time Service

Ref	Level	Owner	Description
53.1.1	L3	Supplier	The Supplier shall provide a time service to ensure all network devices are synchronised to a trusted time source via the Network Time Protocol (NTP).
53.1.2	L3	Supplier	The Supplier shall ensure that the Services are carried out in accordance with the scope and future directions of the NTP set out in the Authority's Technical Framework Document.

53.2 IP Address Management

Ref	Level	Owner	Description
53.2.1	L3	Supplier	The Supplier shall allocate IP addresses for use by the Authority from the Authority's registered class A IP address range or other ranges as nominated by the Authority.
53.2.2	L3	Supplier	The Supplier shall allocate IP address ranges from the Authority's registered class A IP address range to Other Suppliers at their request.
53.2.3	L3	Supplier	The Supplier shall provide a DHCP service for the provision of IP addresses for End User IP telephones at Authority Sites as part of the Voice Services.
53.2.4	L3	Supplier	The Supplier shall maintain the Authority's IP addressing Policy in consultation with the Authority and deliver the Services in compliance with the IP addressing Policy.
53.2.5	L3	Supplier	The Supplier shall provide IP address management for the Authority to include adding, changing, and removing IP addresses at the request of local sites and in support of new and updated site designs.

53.3 Account and Security Administration

Ref	Level	Owner	Description
53.3.1	L3	Supplier	The Supplier shall, as agreed with the Authority, develop, document, implement and maintain Procedures for account and security administration.
53.3.2	L3	Supplier	The Supplier shall perform changes to End User Accounts in accordance with the Service Request management Processes, Policies and Procedures.
53.3.3	L3	Supplier	The Supplier shall perform account and security administration in accordance with the Authority's Information Security Policies and Standards.

53.4 Data Management (Backup, Archive, Restore)

Ref	Level	Owner	Description
53.4.1	L3	Supplier	The Supplier shall, as agreed with the Authority, develop, document, maintain and implement at Authority Premises, service Procedures for data management.
53.4.2	L3	Supplier	The Supplier shall perform data management in accordance with the Supplier's data management Procedures and the Authority's Information Security Policies and Standards.
53.4.3	L3	Supplier	The Supplier shall perform backups and archiving of the Authority Data to a schedule agreed with the Authority and restore data as required, and prior to such agreement in accordance with Good Industry Practice.
53.4.4	L3	Supplier	The Supplier shall provide safe and secure storage of backed up and archived the Authority Data.

53.5 Domain Name System (DNS)

Ref	Level	Owner	Description
53.5.1	L3	Supplier	The Supplier shall provide a DNS service in accordance with the Authority's Technical Framework Document.
53.5.2	L3	Supplier	The Supplier will provide a domain registrar service to register Authority domains and sub-domains with an internet domain name registry in accordance with the Authority domain Process.

53.6 Demilitarised Zone (DMZ)

Ref	Level	Owner	Description
53.6.1	L3	Supplier	The Supplier shall provide a demilitarized zone (DMZ) service in accordance with the Authority's Technical Framework Document.

53.7 Directory Services

Ref	Level	Owner	Description
53.7.1	L4	Authority	The Authority shall provide username, business group, Site location data and other information not available to the Supplier for insertion into the Authority-wide internal Directory Service.
53.7.2	L3	Supplier	The Supplier shall provide the Authority-wide internal Directory Service which shall include but not be limited to, username, business group, Site location, telephone extension number and mobile number) allowing the support of number plan changes within the Authority.
53.7.3	L3	Supplier	The Supplier shall ensure that regular (minimum monthly) updates to the directory information on the allocation of mobile numbers to End Users are obtained from the mobile service provider, with the aim of assisting the Supplier in the delivery of the Directory Services, in accordance with the Technical Framework Document.
53.7.4	L3	Supplier	The Supplier shall update the Authority-wide internal directory on a daily basis, or as otherwise notified by the Authority.

53.8 Dial and Number Plan Management

Ref	Level	Owner	Description
53.8.1	L3	Supplier	The Supplier shall provide the Voice Services in accordance with the Authority's voice dial plan and numbering plan (which shall contain Site access codes, extension number ranges and direct dial in (DDI) numbers) and maintain all the Authority's direct and partial mappings between these numbers and their respective service end points. The Supplier shall not change the Authority's current mappings or dial plan or number plan, unless requested by the Authority to do so.
53.8.2	L3	Supplier	The Supplier shall implement a single numbering plan for telephony for all the Authority's End Users and Sites and ensure that there is a consistent and logical relationship between DDI numbers and initially allocated IP telephone numbers, where reasonably practical.
53.8.3	L3	Supplier	The Supplier shall ensure that individual numbers are allocated to End Users and remain associated with those End Users until such time as the Authority requests otherwise.
53.8.4	L3	Supplier	The Supplier shall ensure that the numbering plan is applied to all Authority Personnel, including those working in Contact Centres.
53.8.5	L3	Supplier	The Supplier shall ensure that the numbering plan supports four (4) digit Site access codes for all Sites.

54. Network Security

54.1 Network Security Management

Ref	Level	Owner	Description
54.1.1	L3	Supplier	The Supplier shall adhere to Schedule 2.4 (<i>Security Management</i>) and the Authority's Information Security Policy and Standards.

55. Network Hardware and Software Provision

55.1 Hardware Maintenance

Ref	Level	Owner	Description
55.1.1	L3	Supplier	The Supplier shall maintain the hardware used in the provision of the Services to ensure that performance and functionality of the Services are maintained in accordance with the Performance Indicators and Target Performance Levels in Schedule 2.2 (<i>Performance Levels</i>).
55.1.2	L3	Supplier	The Supplier shall repair or replace (at the Supplier's option) hardware that develops a fault unless the hardware is a commodity item which is under manufacturer's warranty (excluding telephone handsets). For commodity items that are under manufacturer's warranty, the Supplier shall arrange for the repair or replacement of such commodity items that develop a fault under manufacturer's warranty.
55.1.3	L3	Supplier	The Supplier shall repair or replace (at the Supplier's option) network equipment that develops faults.
55.1.4	L3	Supplier	The Supplier shall proactively maintain hardware used by the Supplier in provision of the Services in order to prevent faults to the extent that it is reasonably possible to prevent such faults.
55.1.5	L4	Authority	In situations where the Supplier has provided the relevant End User with a replacement for a faulty commodity item, the Authority shall connect the replacement item under the instruction of the Supplier.
55.1.6	L4	Authority	The Authority shall report any faults it is aware of in such hardware to the Supplier.

55.2 Managed Equipment Room Service (MERS)

55.2.1 Service Scope

Ref	Level	Owner	Description
55.2.1.1	L3	Supplier	The Supplier shall provide the MERS in respect of all equipment rooms (including all equipment cabinets in those equipment rooms) and free standing equipment cabinets (not in equipment rooms) designated by the Authority plus any additional free standing items of equipment that support the overall service (such as wireless network infrastructure).
55.2.1.2	L3	Supplier	The Supplier shall maintain equipment rooms and equipment cabinets to prevailing UK health and safety Standards, as amended from time to time.
55.2.1.3	L3	Supplier	The Supplier shall notify the Authority of any health and safety hazards which may arise in connection with the performance of the MERS.
55.2.1.4	L3	Supplier	The Supplier shall inform all persons engaged in the performance of the MERS at the Authority-nominated Sites of any hazards notified and instruct such persons in connection with any necessary associated safety measures.
55.2.1.5	L3	Supplier	The Supplier shall advise the Authority's Facilities Management Contractors (FMC) of additional requests for environmental and power requirements from all service towers.
55.2.1.6	L3	Supplier	The Supplier shall reject any Service Requests that would result in existing environmental or power capacities being exceeded in any equipment room or equipment cabinet.

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

55.2.1.7	L3	Supplier	The Supplier shall co-operate and work with the Authority's FMC(s) to ensure that sufficient environmental and power capacities are available for all equipment installed/to be installed in each equipment room and/or equipment cabinet.
55.2.1.8	L3	Supplier	The Supplier shall develop Operating Procedures with the Authority's FMC(s) for the management of environmental and power capacities required for equipment rooms and/or equipment cabinets and provide MERS in compliance with such Procedures.
55.2.1.9	L4	Authority	The Authority shall notify the Supplier of any health and safety hazards which may exist or arise at any Sites occupied by the Authority and which may affect the Supplier.
55.2.1.10	L4	Authority	The Authority shall provide the Supplier with a list of authorised keyholders on a per-Site basis.
55.2.1.11	L4	Authority	The Authority shall ensure that their FMC(s) provide baseline environmental and power capacity information to the Supplier and provide updates of that information from time to time and/or as reasonably requested by the Supplier.
55.2.1.12	L4	Authority	Any works associated with equipment room infrastructure, power or air conditioning shall be implemented by the Authority's FMC(s) and charged direct by them to the Authority.
55.2.1.13	L4	Authority	Inform the Authority employees, agents, Other Suppliers, Site security and third parties of access restrictions that apply to equipment rooms and equipment cabinets and the need to comply with prevailing Standards, Policies and access control Procedures.

55.2.2 Equipment Rooms

Ref	Level	Owner	Description
55.2.2.1	L3	Supplier	The Supplier shall manage the Authority's equipment rooms in compliance with the Authority's standards listed below.
55.2.2.2	L3	Supplier	The Supplier shall work with the Authority to ensure the maintenance of the Authority's technical documentation that is required for the Supplier to provide the MERS.
55.2.2.3	L3	Supplier	The Supplier shall manage equipment cabinet and equipment room space to allow the optimum positioning of IT equipment, in accordance with the Authority's Standards as detailed in Schedule 2.3 (<i>Standards</i>).
55.2.2.4	L3	Supplier	The Supplier shall provide mains power and air conditioning demand volumes for all equipment to be installed in equipment rooms to the Authority's FMC(s) so that they can: a) update air conditioning demand graphs, with projected forward loads and comply with the Authority's spare capacity guidelines; b) update mains power demand graphs, with projected forward loads and comply with the Authority's spare capacity guidelines; and c) update backup power demand graphs, with projected forward loads and comply with the Authority's spare capacity guidelines.
55.2.2.5	L3	Supplier	The Supplier shall label equipment and cables required to deliver the Services to ensure adherence to the Authority's cabling Standards as detailed in Schedule 2.3 (<i>Standards</i>).
55.2.2.6	L3	Supplier	The Supplier shall manage patch leads and maintain patch records to ensure adherence to the Authority's cabling Standards as detailed in Schedule 2.3 (<i>Standards</i>).

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

55.2.2.7	L3	Supplier	The Supplier shall define the access control Procedure for each equipment room (for agreement by the Authority, such agreement not to be unreasonably withheld or delayed), and subsequently maintain an audit trail of access to, and third party works carried out in that equipment room.
55.2.2.8	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that access to equipment rooms is controlled in compliance with the access control Procedure.
55.2.2.9	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that physical access security to the equipment rooms and equipment cabinets is maintained according to the Process for access control act as a reporting point for any breaches or attempted breaches which shall be notified to the Authority as soon as reasonably possible upon discovery.
55.2.2.10	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that the Process for access control is used and maintained for the issue of keys by the keyholders to the Supplier's installation and maintenance staff and those of third party service providers.
55.2.2.11	L4	Authority	The Authority shall ensure that Site security and any other keyholder complies with the reasonable instructions of the Supplier when access to equipment rooms is required and communicates the security Policies of the Authority to any person issued with a key who is not an employee, agent or contractor of the Supplier.
55.2.2.12	L3	Supplier	The Supplier shall ensure that, where equipment cabinets are capable of being locked, keyholders and those Supplier installation/maintenance staff and third party service provider installation/maintenance staff who are issued with a key are made aware of the Authority's security Policies regarding the securing of such equipment cabinets which requires them to be locked following installation and maintenance work.
55.2.2.13	L3	Supplier	The Supplier shall perform the following in respect of each equipment room and each equipment cabinet within such equipment room: a) document equipment room designs pre-implementation and as installed, including photographs and valid electrical certificates (as such certificates are issued by the relevant client); b) maintain and update records of equipment within equipment cabinets and in equipment rooms; c) provide Project work schedules and the co-ordination of Work Requests in connection with works within equipment cabinets and equipment rooms; d) undertake the following work: 1. maintenance and storage of patching records; 2. monthly sample audits of equipment rooms (including all equipment cabinets in those equipment rooms), as identified by the Authority, to ensure Standards compliance, including the notification of non-compliance; e) monitor space and, in conjunction with the Authority's FMC(s), undertake capacity management for environment and power within equipment cabinets and in equipment rooms; and f) track and approve access requests.
55.2.2.14	L3	Supplier	The Supplier shall coordinate third party service providers with regard to their requirements for equipment room access, floor space, equipment cabinet space, power and air conditioning, and communicating such power and air conditioning requirements to the Authority's FMC(s).
55.2.2.15	L3	Supplier	When assessing access requests from third party service providers or when planning to install additional Service infrastructure, the Supplier shall undertake amongst any other necessary tasks each of the following to the extent necessary for the access request or planned installation to be fulfilled:

CONTRACT FOR THE PROVISION OF
IMS4 SERVICES

			a) confirm with the Authority's FMC(s) that adequate access exists for the movement of Service infrastructure into and out of the equipment rooms; b) confirm with the Authority's FMC(s) that adequate mains power exists within the equipment rooms; c) confirm with the Authority's FMC(s) that adequate air conditioning exists, based on the British Thermal Units (BTU) output of the planned equipment, such that manufacturer's guidelines for equipment operating temperature and humidity are not exceeded; d) confirm with the Authority's FMC(s) that the floor loading for any planned Service infrastructure does not exceed the load bearing capacity of the equipment room floor; e) ensure that existing equipment cabinet service areas (front and rear) shall not be compromised by any planned Change; f) ensure that new equipment cabinets shall have adequate service areas allocated (front and rear); and g) inform the Authority's FMC(s) of new equipment cabinet plans so that the FMC can ensure that new equipment cabinets shall not reduce ambient lighting.
55.2.2.16	L4	Authority	The Authority shall ensure that the Authority's FMC(s) provide the Supplier with information on Site and equipment room physical limitations to access, which shall be updated from time-to-time.
55.2.2.17	L4	Authority	The Authority shall ensure that the Authority's FMC(s) provide documentation pertaining to the floor loading potential of each equipment room, when reasonably requested by the Supplier.
55.2.2.18	L4	Authority	The Authority shall ensure that the Authority's FMC(s) maintain ambient lighting levels such that they are not compromised by the addition of additional equipment cabinets, recommending additional lighting to the Authority where this is likely to be the case, and maintain temperatures in accordance with the Supplier's reasonable requirements and at a maximum of twenty five (25) degrees Celsius.
55.2.2.19	L4	Authority	The Authority shall ensure that the Authority's FMC(s) cooperate with the Supplier and comply with the Supplier's reasonable instructions in relation to access requests or installation of additional Service infrastructure.
55.2.2.20	L3	Supplier	The Supplier shall create, maintain and update equipment room documentation that shall include, but not be limited to, the following: a) equipment room floor plans; b) equipment room and equipment cabinet layouts, and cabinet/equipment owners; c) inventories of IT equipment installed in equipment rooms, with sufficient information to identify equipment by equipment cabinet; d) network circuit inventories; and e) cabling patching records.

55.2.3 Free-standing Equipment Cabinets

Ref	Level	Owner	Description
55.2.3.1	L3	Supplier	Where an equipment cabinet is free-standing within an office or other room or space at a Site which is not an equipment room, the Supplier shall ensure that it is included in the MERS along with any other equipment rooms for that Site.
55.2.3.2	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that access to equipment cabinets is controlled in compliance with the access control Procedure.
55.2.3.3	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that physical access security to the equipment cabinets is maintained according to the Process for access control, act as a reporting point for any breaches or attempted breaches which shall be notified to the Authority as soon as reasonably possible upon discovery.
55.2.3.4	L3	Supplier	In conjunction with the Authority's FMC(s) and Site security, the Supplier shall ensure that the Process for access control is used and maintained for the issue of keys by the keyholders to the Supplier's installation and maintenance staff and those of third party service providers.
55.2.3.5	L4	Authority	The Authority shall ensure that Site security and any other Site keyholder complies with the reasonable instructions of the Supplier when access to equipment cabinets is required and communicates the security Policies of the Authority to any person issued with a key who is not an employee, agent or contractor of the Supplier.
55.2.3.6	L3	Supplier	The Supplier shall ensure that where equipment cabinets are capable of being locked, keyholders and those Supplier installation/maintenance staff and third party service provider installation/maintenance staff who are issued with a key are made aware of the Authority's Information Security Policies and Standards regarding the securing of such equipment cabinets which requires them to be locked following installation and maintenance work.
55.2.3.7	L3	Supplier	The Supplier shall perform the following in respect of each equipment cabinet: a) document equipment cabinet designs pre-implementation and as installed, including photographs and valid electrical certificates (as such certificates are issued by the relevant client); b) maintain and update records of equipment within equipment cabinets; c) provide Project work schedules and the co-ordination of Work Requests in connection with works within equipment cabinets; d) undertake the following work: 1. the maintenance and storage of patching records; 2. audit 50% of the total number of equipment cabinets per annum, such that all equipment cabinets will have been audited every two (2) years to ensure standards compliance, including the notification of non-compliance; e) monitor space and, in conjunction with the Authority's FMC(s), undertake capacity management for power within equipment cabinets; f) the tracking and approval of access requests.
55.2.3.8	L3	Supplier	The Supplier shall coordinate third party service providers with regard to their requirements for equipment cabinet access, space and power, and communicating such power requirements to the Authority's FMC.

55.2.3.9	L3	Supplier	When assessing access requests from third party service providers or when planning to install additional Service infrastructure, the Supplier shall undertake amongst any other necessary tasks each of the following to the extent necessary for the access request or planned installation to be fulfilled: a) ensure that existing equipment cabinet service areas (front and rear) shall not be compromised by any planned Change; b) ensure that new equipment cabinets shall have adequate service areas allocated (front and rear). c) create, maintain and update equipment cabinet documentation that shall include, but not be limited to, the following: d) equipment cabinet layouts, and cabinet/equipment owners; e) inventories of IT equipment installed in equipment cabinets, with sufficient information to identify equipment by equipment cabinet where more than one equipment cabinet is co-located; f) network circuit inventories, where relevant; g) cabling patching records.
----------	----	----------	---

55.3 Software Distribution

Ref	Level	Owner	Description
55.3.1	L3	Supplier	The Supplier shall perform software distributions for the Services in accordance with the release management Processes, Policies and Procedures.

55.4 Software Maintenance

Ref	Level	Owner	Description
55.4.1	L3	Supplier	The Supplier shall maintain the software provided and used by the Supplier in the provision of the Services to ensure Target Performance Levels, functionality and performance of the Services are maintained.
55.4.2	L3	Supplier	The Supplier shall apply security patches approved by the Authority to the software in accordance with security Policies.

56. Network Maintenance and Software Provision

56.1 Deskside Support

Ref	Level	Owner	Description
56.1.1	L3	Supplier	The Supplier shall provide on-Site installation, configuration, Incident resolution and repair of the network services.

56.2 Installs, Moves, Adds, Changes and Deletions (IMACDS)

Ref	Level	Owner	Description
56.2.1	L3	Supplier	The Supplier shall deliver all deskside support to End Users as required in the performing installs, moves, adds, changes and deletions for any aspect of network services.

57. Additional On-Demand Services

57.1 Consultancy Services

Ref	Level	Owner	Description
57.1.1	L3	Supplier	If requested by the Authority, the Supplier shall provide network related professional and consultancy services on a daily basis against a set of agreed charge rates for Project work, including feasibility studies.

57.2 Training services

Ref	Level	Owner	Description
57.2.1	L3	Supplier	If requested by the Authority, the Supplier shall provide training for selected Authority staff ('train the trainer') within each the Authority business groups as part of the deployment and provision of the Services. The aim of this is to enable such Authority staff to then train End Users of the Services to make full use of the Services.
57.2.2	L3	Supplier	If requested by the Authority, the Supplier shall agree the detailed nature, timing and quality of the training provided as part of the 'train the trainer' consultancy with the Authority as part of a training needs analysis and document this in a training strategy. The Supplier shall ensure that the training strategy addresses the following areas, as a minimum: a) needs analysis; b) target audience; c) development of course structure and content; d) communication plan for courses; e) training programme (course titles, trainers, suitability, duration, dates, locations); f) learning materials; and g) evaluation of training effectiveness.

Cloud Hosting Support Services Services Descriptions

58. Hosting of Applications

58.1 Hosting of Applications

Ref	Level	Owner	Description
58.1.1	L3	Supplier	The Supplier shall manage a cloud-hosting capability for Authority Services, where required, in accordance with the Authority's Technical Framework Document.
58.1.2	L3	Supplier	The Supplier shall maintain any hosted resources in accordance with the cloud vendor's support and security guidance.
58.1.3	L3	Supplier	The Supplier shall operate any cloud-hosting environments in accordance with the Authority's Information Security Policy and Standards and in accordance with the Technical Framework Document.
58.1.4	L3	Supplier	The Supplier shall support and manage the cloud hosting of in-scope services, cost effectively, within their scope, including but not limited to areas such as auto-provision and auto-scaling.
58.1.5	L3	Supplier	The Supplier shall manage the cloud hosting platforms using the Authority's cloud management platform tools.
58.1.6	L3	Supplier	The Supplier shall deliver a managed orchestration capability for their Services, within the Supplier and with other third party providers where appropriate.
58.1.7	L3	Supplier	The Supplier shall provide scheduling and implementation of required Updates and patches to the hosting environment, co-ordinating as appropriate with the Authority, and to minimise impact to the availability of the Services.
58.1.8	L3	Supplier	The Supplier shall be responsible for the maintenance, and creation of new where required, hosting resource configuration and Policies, in accordance with the Authority's Policies, Processes and Standards as applicable, e.g. Role Based Access Control (RBAC).
58.1.9	L3	Supplier	The Supplier shall manage the hosting audit log in accordance with the Authority's Policies for data retention.
58.1.10	L3	Supplier	The Supplier shall provide configuration and support of the cloud hosting backup service in accordance with the Authority's Production Control Procedures.
58.1.11	L3	Supplier	The Supplier shall provide the capability to undertake ad-hoc backups of the cloud hosting services and agree the Process for the provision of this activity with the Authority.
58.1.12	L3	Supplier	The Supplier shall carry out regular checks on the success of backups, and perform Test restores to ensure the data is recoverable when required.
58.1.13	L3	Supplier	The Supplier shall ensure that an automated failover capability is configured for the cloud hosting services where agreed with the Authority and in accordance with the Authority's Change Management Policies and Processes.
58.1.14	L3	Supplier	The Supplier shall be responsible for the identity management of End User Accounts and role-based access for cloud hosting services within their scope.
58.1.15	L3	Supplier	The Supplier shall provide configuration, maintenance and support of the infrastructure as code in accordance with the Authority's Production Control Procedures.
58.1.16	L3	Supplier	The Supplier shall undertake infrastructure as code management to ensure the configuration is maintained as the service evolves over time as part of managed change to the Service.
58.1.17	L3	Supplier	The Supplier shall provide configuration and maintain the monitoring capability of the cloud hosting services within their scope, in accordance with the Authority's Production Control Procedures.

58.1.18	L3	Supplier	The Supplier shall provide ongoing improvements and enhancements to the monitoring services for cloud hosting as agreed with the Authority.
58.1.19	L3	Supplier	The Supplier shall provide regular information to the Authority against the consumption of cloud hosting services and provide trend analysis against capacity planning.
58.1.20	L3	Supplier	The Supplier shall provide validation of and information against the Charges incurred for cloud hosting services and ensure that analytics and recommendations are provided to improve the future consumption and cost reduction of services within their scope.

58.2 Gated Governance

Ref	Level	Owner	Description
58.2.1	L3	Supplier	The Supplier shall support the preparation of information related to the provision of Services and required by the Authority for the Gated Review Process and in alignment with the Office of Government Commerce's Projects In Controlled Environments (PRINCE2), Managing Successful Programmes (MSP) or any agile methodology as required by the Authority, and in accordance with Schedule 2.3 (<i>Standards</i>).

58.3 Implementation Planning

Ref	Level	Owner	Description
58.3.1	L3	Supplier	The Supplier shall agree with the Authority the implementation plan for each new or changed application or New Release.
58.3.2	L3	Supplier	The Supplier shall comply with its obligations pursuant to each agreed implementation plan.

58.4 Transition Management – Per Release

Ref	Level	Owner	Description
58.4.1	L3	Supplier	The Supplier shall engage in and support the transition management process.

58.5 Pilot Testing

Ref	Level	Owner	Description
58.5.1	L3	Supplier	The Supplier shall produce, maintain and provide to the Authority pilot Test Plans where required.
58.5.2	L3	Supplier	The Supplier shall participate in the execution of pilot Testing including re-Testing and regression Testing as necessary, in accordance with Schedule 6.2 (Testing Procedures)..

Future Services

59. Future Services

59.1 General

59.1.1 The Supplier acknowledges that nothing in this Paragraph 59 shall oblige the Authority to take any Future Services from the Supplier or prevent the Authority from receiving services or projects similar or identical to the Future Services from any third party.

59.1.2 The Supplier shall, at all times during the Term:

- (a) provide all Future Services requested by the Authority in accordance with this Agreement (provided that such request complies with this Paragraph 59); and
- (b) ensure that it is able to provide Future Services as requested by the Authority in accordance with this Paragraph 59 without any risks or impacts (including any arising in connection with the Implementation, Testing or operational use of such or Future Services) to:
 - a. the rights and obligations of either Party under this Agreement; and
 - b. to the provision of Goods and Services by the Supplier to the Authority in accordance with this Agreement (each a "**Risk/Impact**").

59.1.3 The Supplier shall ensure that, at all times during the Term, the Future Services comply with all requirements applicable to the Goods and Services (including as set out elsewhere in this Agreement).

59.2 Calling-off Future Services

59.2.1 The Authority may notify the Supplier that it requires any Future Service by issuing a Contract Change Request to the Supplier in accordance with the Change Control Procedure.

59.2.2 Subject to Paragraph 59.2.4 of below, the Parties shall follow the Change Control Procedure to agree the provision of the Future Service, which shall include documenting, in respect of the relevant Future Service:

- (a) any additional or variant terms and conditions;
- (b) the Authority Requirements;
- (c) Milestones and an Implementation Plan (in accordance with Schedule 6.1 (*Implementation Plan*));
- (d) the Testing procedures (in accordance with Schedule 6.2 (*Testing Procedures*));

- (e) any additional Charges (in accordance with Schedule 7.1 (*Charges and Invoicing*));
- (f) performance levels (in accordance with Schedule 2.2 (*Performance Levels*));
- (g) any applicable Change to this Schedule;
- (h) any applicable Change to Schedule 8.5 (*Exit Management*); and
- (i) any applicable Change to Schedule 11 (*Processing of Personal Data*).

59.2.3 In addition to the obligations set out in Schedule 8.2 (*Change Control Procedure*), the Supplier shall, as part of the Impact Assessment provided by the Supplier in relation to such Contract Change Request:

- (a) without prejudice to Paragraph 59.1.2 above, inform the Authority of every Risk/Impact (and potential Risk/Impact) and how it proposes to mitigate or remove such Risk/Impact; and
 - (b) promptly provide all information and assistance necessary to enable the Authority to assess the nature, risk or impact of any Risk/Impact (or potential Risk/Impact) or any proposal made by the Supplier under Paragraph 59.2.3(a) above.
- 59.2.4 Notwithstanding any provisions of Schedule 8.2 (*Change Control Procedure*), the Supplier acknowledges and agrees that if a Future Service is called-off by the Authority in accordance with this Paragraph 59.2, any failure by the Supplier to implement, Test and commence the provision of a Future Service shall be a Default by the Supplier.

59.2.5 The Supplier shall, at no additional cost to the Authority, implement and commence provision of any other services, functions and responsibilities which are either necessary for, or incidental to, the proper performance by the Supplier of the Future Service.

59.2.6 The Future Services are set out in Paragraphs 59.3 to 59.5 below.