SCHEDULE 2.1 SPECIFICATION FOR WIDE AREA NETWORK FOR BCP COUNCIL

CONTENTS

1. INTRODUCTION 2
2. NETWORK MANAGEMENT 4
3. TRANSITION AND IMPLEMENTATION ARRANGMENTS 9
4. ICT SERVICE REPORTING AND SERVICE REVIEW 15
5. SERVICE AND SERVICE DESK MANAGEMENT 20
6. CONFIGURATION AND CHANGE MANAGEMENT 25
7. ICT PROCUREMENT SERVICE 28
8. CAPACITY PLANNING/PERFORMANCE MONITORING 29
9. INFRASTRUCTURE MAINTENANCE 30
10. SECURITY MANAGEMENT 31
11. FUTURE PROJECT CONSIDERATIONS – SERVICE DEVELOPMENT 34
12. ANNEX A TO SCHEDULE 2.1 37

READ-ONLY

1. INTRODUCTION

1.1. This Schedule details the requirements of Bournemouth Christchurch and Poole (BCP) Council (the Council) for the provision of a new Wide Area Network (WAN) and supporting services. The Supplier shall develop their solutions to either meet or exceed these requirements.

1.2. The Council is intending to identify a single Supplier for the provision of a Wide Area Network, Internet Breakout Connectivity, Microsoft Express Route and supporting Service Management. The successful Supplier is required to provide all the software, hardware, connectivity, configuration and support (including necessary training) that meet the requirements outlined by the Council, within agreed critical lead times. It is essential that the Supplier delivers a flexible service, with emphasis on scalability to meet the future IT requirements and service provision of the newly merged BCP Council.

1.3. BCP Council has resulted from a merger of Bournemouth Borough Council, Christchurch Borough Council and the Borough of Poole undertaken on 1 April 2019 as part of a larger Dorset restructure. BCP Council has approximately 6000 staff based in 83 locations around the Council.

1.4. The IT Strategy for BCP Council aims to take advantage of new technology to enable greater business efficiency and improved service delivery. Examples of some of the ongoing projects are:

- Migration to Office 365
- Deployment of Skype for Business
- Cloud first program of works based on the Microsoft Azure platform
- LAN replacements for Bournemouth and Poole alongside a Wi-Fi refresh.
- Telephony system replacement.
- Mobile Working

1.5. As part of the IT Strategy, the Council wishes to implement a Wide Area Network (WAN) in order to implement and support the above projects and minimise the current Supplier base (currently multiple Internet Service Providers (ISPs)). It is vital that the WAN meets all the requirements below in order to deliver an effective IT Strategy for BCP Council.

1.6. The BCP LAN comprises of products from the Extreme Networks portfolio including:

- VSP 8404 Core Switches
- ERS 4900 Series Data Centre and Edge Switches
- X440-G2 Edge switches

1.7. The Councils Local Area Network (LAN) uses Extreme Fabric Connect technology to create a backbone Link between the L3 Core & L2 edge using MAC in MAC encapsulation, this technology requires an MTU of 1600 to work and it is desirable for the Supplier's Wide Area Network (WAN) to be able to support this technology.

1.8. The devices also support the OSPF protocol if the fabric technology cannot be incorporated into the WAN.

1.9. The BCP Datacentre (DC) will be comprised of three separate DC's which will be virtualised using the Extreme Fabric technology. If this cannot be done over the WAN Link, a series of separate 10Gb Links must be provided to form a resilient triangle between the three main DC buildings.

READ-ONLY

Scope

1.10. The Council is seeking a Supplier to provide a Wide Area Network (WAN), Internet Breakout Connectivity, Microsoft Express Route connection and Support Service Management.

1.11. Where it is stated 'service management' of a service this includes, but is not limited to proactive monitoring, reporting, as well as corrective and preventative action.

1.12. The Council requires the delivery of the services in accordance with all of the relevant requirements set out in this Schedule.

1.13. The Supplier is fully responsible for the undertaking of any site visits under due diligence to ensure they accurately understand the Council's requirements and price accordingly. The Council will not accept any variations on price where the Supplier has failed to undertake sufficient enquires and investigation in order to price correctly.

1.14. The Supplier shall be responsible for delivering the following elements:
   (a) Wide Area Network (WAN) - currently 86 connections across 83 sites;
   (b) Internet Breakout Connectivity;
   (c) Microsoft Express Route;
   (d) Supporting Service Management;

1.15. The Council reserves the right to add or remove sites during the length of the contract as business demands change which may affect the requirements for the WAN service. Suppliers will need to ensure that their design as well as service delivery model is able to manage the addition and removal of sites during the term of the contract.

1.16. It is intended that the Supplier will begin the implementation of the Wide Area Network (WAN) and other required services in late 2019. The commencement date of the contract will be at the point the implementation team (Suppliers Project Team) is formed.

1.17. The Supplier will be required to install the WAN as soon as possible. The Council will only pay rental and support fees once a Link is installed, tested and signed off by the Council. The Council requires the billing to be consolidated and quarterly in arrears, in total for all circuit charges and support. The quarterly invoice should list all circuits individually, so the Council can easily monitor expenditure.

1.18. When each Link is installed, this will commence the Service Start Date for that Link. Each Link will have a Service Period of three years, each starting on the Service Start Date for that Link. There will be the ability with each Link to extend the Service Period for up to four years. Therefore, if all extensions were taken, the full length of the contract would be for up to 7 years per Link.

READ-ONLY

2. NETWORK MANAGEMENT

2.1. Objectives of the Contract

2.1.1. In performing its obligations under the Contract, the Council will be looking for the Supplier to work towards the following objectives:

a. Minimise the costs associated with the WAN / Internet connectivity;
b. Increase network availability and resiliency;
c. Improve the quality of service being provided to the wider Council;
d. Provide future flexibility and security as network services evolve;
e. Enhance levels of services with respect to technical coverage;
f. Obtain leading edge pricing and terms and conditions for the period of the contract;
g. Implementation of Microsoft Express Route within the WAN solution;
h. Implementation of Internet Breakout within the WAN solution.

2.2. Design / Solution

2.2.1. **Service Supply –** The Supplier will provide the services from the commencement date and shall ensure that all the services;

- Comply in all respects with the specification requirements;
- Are supplied in accordance with the Supplier's service descriptions and the terms of the agreement;
- Do not prejudice the Council's compliance with, or cause the Council to breach, the Code of Connection and / or Public Services Network (PSN) / Payment Card Industry (PCI) compliance certification.

2.2.2. **Solution Architecture** – for the WAN, Internet Connectivity and Microsoft Express Route the Council requires the Supplier to produce:

- A Technical Architecture
- An overall topology diagram of their proposed design, which includes the WAN, Internet Breakout circuit and Microsoft Express Route connection.

2.2.3. Prior to implementation the Supplier will be required to provide detailed documentation, including:

- Technical Architecture
- Security Architecture
- Service Levels and Service Management Procedures

2.2.4. **Scalability -** The Supplier solution must have the ability to react to:

- Growth in the number of sites
- Growth in the number of services deployed and service utilisation e.g. increase in the use of cloud-based services or remotely hosted services
- Decrease in the number of sites or change in function
- The ability of the contract (therefore cost) to react to change

2.2.5. **Diversity and Resilience / Redundancy** – For the WAN, Internet Connectivity and Microsoft Express Route, the Council will require the Supplier to deliver:

The Core layer;

READ-ONLY

- A multiple PoP architecture
- Each device is housed in a separate building
- Ensuring genuine device separation
- Redundancy within the design

The Distribution layer;

- A multiple layer architecture
- Inter-site resilience and bandwidth
- Redundancy within the design

The Aggregation layer;

- A multiple layer architecture
- Resilience and bandwidth
- Redundancy within the design

Identification if the service provisioned is based on:

- Resilience (Active / Passive)
- Load Balanced

2.2.6. **Protocols and Protocol Management** – The Supplier will be required to employ current and future protocols and network traffic management protocols including those detailed below:

- **IPV4 and IPV6 -** Support for both IPV4 and IPV6 addressing standard
- **QOS –** Support Quality of Service (QoS) across the solution
- **COS –** Support traffic prioritisation based on Class of Service (COS)
- **BGP –** Support for exchange routing and reachability
- **ISIS –** Support of Extreme Fabric Connect and Fabric Attach
- **VRF –** Support for Virtual Routing and Forwarding
-

2.2.7. **Single Point of Failure (SPOF)** – The Supplier must ensure that through the future provision of a network architecture design, that there are no Single Points of Failure (SPOF) within all core elements of the WAN, Internet solution and Microsoft Express Route.

2.2.8. **Core Network Resiliency** – The Suppliers design must be fully resilient between the three main sites: Bournemouth Town Hall, Christchurch Civic Centre and Poole Civic Centre. This resiliency must support virtualised datacenter using Fabric Technology, even if this means having two different types of circuits, one for WAN and one for VDC, and must have minimum 10GB Links.

2.2.9. **Internet Breakout Connectivity –** The Supplier is required to develop a method for achieving internet breakout connectivity from within their WAN via a 1GB minimum connection. The Council requires the ability to install dual Checkpoint 5800 Firewalls within the Suppliers designated datacenter to control internet access. The Council requires remote access for configuration tasks and general operating purposes.

2.2.10. **Microsoft Express Route –** The Supplier is required to achieve connectivity from their WAN for the provision of a Microsoft Express Route as part of the solution, therefore enabling a private connection between the Azure data centers and the Councils “infrastructure”. This will then enable the Council to experience greater reliability, increased connection speeds, lower latencies and improved higher security when compared to a typical Internet connection. The Supplier will be required to directly provide (or enhance) the SLA / KPI metrics that Microsoft apply to the Express Route connection.

READ-ONLY

2.2.11. **Life of System** – The communication system design and principles shall have a potential lifetime of at least seven years from acceptance of the system. Although there may be a requirement to upgrade or withdraw parts of the WAN as the Council expands or changes, and to keep up with ongoing developments, the general architecture adopted will be selected with a view to satisfying the Council's needs over the estimated next seven years.

2.2.12. **Fabric Connect Technology** – It is desirable for the Supplier's Wide Area Network (WAN) to support Extreme's Fabric Connect technology.

2.2.13. **Applications** - The Suppliers solution must be able to support the following Applications (but not limited to) as a minimum:

- Microsoft Office 365
- Skype for Business
- Cloud Applications specifically MS Azure
- IP and Cloud Telephony.
- IP and Cloud Contact Centre applications.
- Mobile working
- CCTV Traffic

2.2.14. For the avoidance of doubt the Council shall be the design authority for the overall network and IPT infrastructure.

2.2.15. The Supplier shall be responsible for all Installs Moves and Changes (IMACs). The Council defines a hard IMAC as requiring physical onsite presence and a soft IMAC being capable of execution via software tooling and remotely. The Supplier must ensure that they have effective processes and procedures and an SLA for IMACs and in particular ensuring:

- Service Element
- IMAC Type (e.g. Soft or Hard)
- IMAC Description
- Differentiation
- Completion Target

The Supplier shall:

(a) provide a full end to end network management service including the management of third party in accordance with the agreed problem resolution procedures and processes as defined by the Council;
(b) provide pro-active network and infrastructure monitoring and support on a 24x7 basis;
(c) provide incident and problem logging, management and resolution;
(d) provide a telephony IMAC service as per the definition of work covering IMAC activities;
(e) develop and maintain the network infrastructure to ensure availability of ICT systems across the Council network to the agreed performance standards;
(f) undertake change configuration of network as authorised by the change management procedure;
(g) carry out capacity planning and monitor and resolve slow performance and undertake quarterly identification of performance bottlenecks, trends, capacity issues and risks;
(h) maintain full documentation including configuration files, details of active components and configuration, network topology, and other relevant network documentation, readily and easily accessible when required by the Council;
(i) provide standard reports detailing availability, health and utilisation of the Council estate;
(j) deliver configuration management to enable effective control of the active network components;

READ-ONLY

(k) act as the first point of contact and responsible owner of third-party connectivity issues;
(l) procure and warrant all new cabling necessary to support the Council's services;
(m) accommodate the Council's requirement to provide secure connectivity and provide the required level of security in accordance with the Council's data sharing policies and other relevant standards.

2.2.16. The Supplier shall take a holistic view when managing a converged environment in order to resolve service faults in a converged system. The Supplier shall have tools specifically designed for this type of environment. These tools shall enable the Supplier to ensure that Council is receiving a network service appropriate to its specific application requirements at that time. Change activity shall be similarly unified in its approach.

2.2.17. The Supplier's system management tools shall provide proactive 24 hours per day seven days per week automated monitoring of the communications infrastructure status, performance against pre-defined thresholds, or alerts / event that indicate a potential to impact the service. The Supplier shall raise an incident where the pre-defined threshold is exceeded or an alert / event is detected. Additionally, Council can raise incidents via the Supplier service desk.

2.2.18. A request for change shall mean a request for a modification to the communication infrastructure which can be completed remotely (typically requests for change are defined as minor or soft) and do not require resources or equipment such as: Consultancy, project management or implementation resources. Additional hardware or software. Requests for change that require resources or equipment as detailed above shall be processed as a service request. The Supplier shall validate that the change requestor is an authorised Council representative.

2.2.19. The Supplier shall undertake appropriate risk assessment, planning and develop backup, regression and test plans for all major and significant requests for change. The Supplier shall update the network documentation to reflect the request for change once the request for change is completed.

2.3. **Documentation Management**

2.3.1. The Supplier shall maintain a database which details the current hardware and software specification for each managed communications infrastructure device. The Supplier shall also maintain up to date documentation as detailed in the table below:

Document	**Description**	**Format**
High Level Topology	This high-level topology diagram shall show the major sites in the Council network and their interconnection	TBA
Detailed Topology	A diagram or diagrams showing all network devices, common names, links and link speeds and IP addresses of each interface.	TBA
Network Bandwidth Details and Suppliers	Shall contain details of each link, with the carrier, link size and operating parameters such as CIR & port speeds.	TBA

2.3.2. The Supplier shall ensure that all documentation and software configurations held on the Supplier management systems are backed up regularly and backups of the latest versions

READ-ONLY

shall also be stored in a secure off-site location for the duration of the agreement, and available to authorised Council representatives. Interpretative reports shall be provided on a quarterly basis, whilst real-time reports shall be available at any time to nominated Council representatives.

2.4. **Lifecycle Management**

2.4.1. The Supplier shall work with the Council to manage the availability, performance and utilisation of the infrastructure.

2.4.2. The Supplier shall undertake such monitoring and management arrangements in respect of Network management as defined by the Council in accordance with the Council's governance arrangements and:

(a) Provide quarterly availability and capacity reports.
(b) Attend strategy and planning meetings on a quarterly basis.
(c) Provide ongoing advice via regular scheduled conference calls to the Council, at the Council's request in respect of the communications infrastructure availability, performance, utilisation and capability to support new applications and business initiatives.

2.4.3. The following responsibility matrix specifies in further detail the respective roles and responsibilities of each party:

Roles and Responsibilities	**Supplier**	**Council**
General Responsibilities for Network Management		
1. Define services and standards for environment	**X**	**X**
2. Review and approve services and standards for network environment		**X**
Planning and Analysis		
3. Define functional and service requirements		**X**
4. Participate in defining services and standards for planning and analysis activities	**X**	
5. Review and approve services and standards for planning and analysis activities		**X**
6. Recommend policies and procedures to implement planning and analysis activities	**X**	
7. Review, authorise, and approve policies and procedures		**X**

The Council shall:

(a) use reasonable endeavours to ensure the outgoing provider(s) shall provide all reasonable assistance with the transfer of management and support responsibility to the Supplier or its subcontractor(s);
(b) provide, or procure from its outgoing provider(s), accurate documentation for the legacy network (including IPT, LAN, WAN, analogue and digital voice services); and
(c) ensure that management policies are in place to restrict unauthorised changes, such as rogue access points.

READ-ONLY

3. TRANSITION AND IMPLEMENTATION ARRANGMENTS

3.1. General Provisions

3.1.1. If at any time, for any reason and regardless of whose fault the Supplier considers the delay to be, the Supplier becomes aware that it will not (or is unlikely to) achieve any milestone and/or test by the milestone date it shall:

- Immediately notify the Council in writing of the fact and likely length of such delay and summarise the reasons for it.
- Immediately notify the Council of the consequences or likely consequences of such delay
- Immediately notify the Council in the form of a "correction plan" the actions being undertaken to achieve the deliverables outlined against the milestone, dates as to when it will be achieved and a brief statement as to how the milestones deliverables will be achieved.
- Mitigate the impact on the Council of such delay.

3.2. Implementation Plan

Draft Implementation Plan – 15 Working Days

3.2.1. No later than 15 working days from the effective date of a resulting contract, the successful Supplier will provide a detailed draft Implementation Plan that sets out:

- Implementation timing;
- Milestones;
- Activities/tasks;
- Dependencies;
- Process and individual implementation steps required to implement the services on a site by site bases, covering all key services currently operational at each site.

For Information

3.2.2. The Supplier shall be responsible for all development, updates and maintenance of the Implementation Plan using a project management tool. The Council's preference is for the Supplier to use Microsoft Project software as its project management tool and the wider Microsoft Office suite of applications.

3.3. Detailed Implementation Plan

3.3.1. It is proposed that once the final detailed Implementation Plan has been agreed in writing, it may only be changed at Council discretion. It is noted that the detailed implementation plan is expected to be a working document and will continue to be updated and refined throughout the implementation project.

3.3.2 The priority of the sites to be installed are outlined within the Pricing Schedule document that lists all of the Council's sites. Within this document it states the required Service Start Date that the WAN must be live from.

3.3.3. The Supplier will be required to provide a high-level representative Implementation Plan as part of its tender to demonstrate its understanding of the Council's requirements. The Implementation Plan must clearly identify tasks that the Supplier expects the Council to undertake and the Council's obligations and the timeline that Supplier believes is appropriate for the implementation (measured from the effective date of a resulting contract).

READ-ONLY

3.3.4. The Implementation Plan should detail key stages, dependencies, critical path and the activities required to implement the services identified in this specification to meet the required Service Start Date for each of the Links to be installed. The Supplier must indicate the skill levels required to accomplish the Service Start Dates and which Key Personnel are associated with each skill level.

3.3.5. Any failure by the Supplier to meet the required Service Start Date for each of the Links will result in significant cost for the Council related to the outgoing Supplier, and therefore the Council requires reasonable notice of not less than one calendar month of any potential failure to achieve the Service Start Date to enable the Council to manage costs and decommissioning plans.

3.3.6. The Supplier must advise the Council on a regular basis (to be agreed) of progress against the agreed Implementation Plan. However, any slippage in the program or the occurrence of problems, which might impact the delivery timescale, shall immediately be brought (in writing) to the attention of the Council's implementation manager. In addition, the Supplier will respond promptly to all reasonable requests from the Council or its appointed representative for information to allow an assessment to be made of project progress.

3.3.7. The Supplier shall provide details of lead times and task dependencies for equipment and services to be implemented by location and region within their implementation plan.

3.3.8. The Supplier will be required to ensure that through their implementation processes and procedures, criteria for acceptance and automated tools to be used during the implementation are effective to ensure the Council's internal ticketing and other IT service management systems platform is kept up to date during the implementation (e.g. e-mail versus full electronic Links).

3.3.9. The Supplier is required to ensure that they have effective processes and tools for the delivery of the implementation of service through to support, including the updating of configuration control and device management.

3.3.10. The Supplier must ensure that they have effective processes and policies for coordinating with third parties, their restrictions and flexibility regarding support for transition performance outside of normal working hours and their processes for implementing requested or required changes for the delivery of this service.

3.4. **Project Management**

3.4.1. The Supplier must appoint a senior project manager accountable for managing all Supplier resources, ordering and delivery of equipment, software and other essential project components, through to project acceptance. The Supplier's project manager will form the principal point of contact with the Council's implementation manager for the project. The Council reserves the right to reject candidates if it considers that the person or persons proposed does not have the appropriate skills and/or experience to carry out the proposed work. The Council will not exercise this right unreasonably.

3.4.2. The Suppliers' project manager must be contactable by the Council at all reasonable times and, in the event of his/her absence, a deputy of similar seniority level will be available. At the commencement of the project, the Supplier must advise the Council of the senior personnel within the project team. These personnel shall not be changed without the prior knowledge and agreement of the Council.

3.4.3. The Suppliers project manager will be expected to comply with the PRINCE2 industry standard for project management or equivalent.

READ-ONLY

3.4.4. The Council's project manager will carry out/manage the tasks set by the Supplier's project manager using the Council's resources as recommended by the Supplier. The Council's project manager will therefore be managing the day to day activities (of the Council's resources) but under the stewardship and leadership of the Supplier's project manager.

3.4.5. The Supplier is required to identify any information or resources that the Council will be required to provide to the Supplier in order to complete the implementation.

3.5. **Project Team - 10 Working Days**

3.5.1. Within 10 working days from the effective date of a resulting contract, the Supplier will have its implementation project team ready and prepared to meet with the Council's implementation team in order to establish an understanding of project deliverables, timelines, and individual team member roles and responsibilities.

3.5.2. The Supplier is required to identify their project management team and resources ensuring that the team have relevant experience on the deployment of similar solutions. This is to ensure the successful delivery of the services.

3.6. **Documentation**

3.6.1. There will be a requirement for the provision of project management, user and technical documentation to support implementation of the solution and ongoing operation (all documentation must be provided in Microsoft Office Format). The Supplier will be required to provide a:

- Statement of Works (SOW) including a detailed project and quality plan
- Implementation Plan
- Technical Design Specification
- Technical Solution Documents
- Acceptance Test Specification

3.6.2. The Statement of Works (SOW) should contain a project plan recorded in MS Project and should be regularly updated and available to the Council for monitoring progress. The SOW will clearly identify the resources to be deployed by the Supplier. Once the SOW is agreed, changes shall only be made with the prior written consent of the Council. The Supplier should indicate how the burden on the Councils staff is to be minimised.

3.6.3. Following contract award the implementation plan must be updated with all achievements and progress on a regular basis with regular or exception reports on any task/activity not running to the planned schedule. Plans for changeover/migration including training, pilot or parallel running and acceptance testing (including any recommended staged delivery and testing) must also be provided. The detailed project plan should be provided with the following components:

- Confirmation and quantification of resources for all significant activities and tasks
- Target schedules for all task and activities, with on-going progress recorded
- Responsibilities (of both the Supplier and the Council)
- Project milestones
- Review points
- Elapsed time

READ-ONLY

3.6.4. Following contract award, the Supplier must provide a Technical Design Specification to the Council for approval. Once the Technical Design Specification has been agreed, this shall form the design reference against which the system will be implemented. This document must include as a minimum the following components:

- A description of all the hardware and software to be provided
- A description and diagrammatic representation of how this will fit within the Council's infrastructure.
- A description of how the entire system will operate.

Following contract award, the Supplier must provide a Technical Solution Document that provides comprehensive documents describing the operation of the system.

3.6.5. **Acceptance Test Specification -** For each major part of the proposed solution, the Supplier must provide the Council with an Acceptance Test Specification (ATS). The ATS will be designed to rigorously test all functions defined in the Technical Design Specification

3.6.6. **Testing (Pre-Production) -** The Supplier will be responsible for testing the new equipment prior to its cutover into the Council's production environment. The Supplier will also perform any end-to-end testing to ensure the new equipment is interoperable with connected equipment or transport services

3.7. **Site Implementation Packages**

3.7.1. With respect to sites where new equipment and/or services are to be installed, the Supplier will be required to provide details of what specific preparation is necessary for each site four (4) weeks before the planned date for commencing the installation of equipment at each site. This document is referred to as the Site Implementation Package for a site or site(s) and it will include:

- The final confirmed date(s) for equipment installations;
- All environmental requirements for Supplier-provided equipment;
- Floor space and rack unit requirements;
- Supplier name(s) that will be supplying the shipments of any equipment;
- All third-party Supplier name(s) that will be supplying any services other than the Supplier;
- Documentation of the specific implementation steps for the site;
- A written test plan for the services to be implemented at the sites;
- A written back-out plan for the services to be implemented at the sites.
- The Supplier must describe the acceptance testing that it will perform for different types of service components (e.g. data network services, WAN, Internet Connectivity and Microsoft Express Route services).

3.8. **Acceptance Testing Procedure**

3.8.1. Once the Supplier has completed its acceptance testing it will be required to notify the Council verbally and in writing (email will suffice) that the circuit/service is activated and ask for the Council's acceptance which will also be provided verbally and in writing. The Supplier will also agree that the Council will not be required to pay for any service components that, although accepted, the Council cannot practically use because of other Supplier dependencies.

3.8.2. For Clarification; Each party shall bear its own costs in respect of acceptance testing. However, if a milestone and / or test does not achieve the acceptance criteria the Council shall

READ-ONLY

be entitled to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-testing to achieve the acceptance testing criteria.

3.8.3. Acceptance testing will be carried out by the Council, once the solution (or components thereof) have been handed over by the Supplier and will test the solution functionality as claimed by the Supplier in their Tender response, or any subsequently agreed requirement definition documentation. The Suppliers staff may be present during the acceptance test.

- Acceptance testing must be completed by the Council without any failures before sign-off.
- All documentation must have been handed over to the Council before sign-off.
- All failures and disputes will have been resolved with signatures from all relevant parties before sign-off.
- In the event of a component failing the acceptance test, the Supplier will be given the opportunity to correct the fault within 10 working days and re-submit the component for another acceptance test (to be run in full or in part at the Council's discretion).
- In the event of a component not being corrected within 10 working days, or the acceptance test failing a second time, then at the Council's discretion the Supplier must correct the fault and re-submit the component for a further Acceptance Test or negotiate a reduced cost for the component being supplied.

3.8.4. Further details on the required Acceptance Testing Procedure can be found within Schedule 2.3 – Testing Procedure.

3.9. **Installation**

a. The Supplier will be required to produce a full risk assessment and method statements for the installation of all aspects of their proposed solution.
b. The Supplier shall be responsible for installing and commissioning any new system. It is expected that some installation and testing will be required outside of normal office hours.
c. The Council operates a formal change management process (based on the Information Technology Infrastructure Library (ITIL) framework), to control any changes made to the ICT infrastructure.
d. In support of the Council's change management process, the Supplier must provide the following details for any change made to the Council's IT infrastructure for which they are responsible:

- Technical description of change
- Technical test plan
- Back-out plan
- Risk assessment

e. The Supplier must propose a strategy which will allow the smooth migration from the existing WAN to the replacement WAN without loss of service including voice or data traffic and without any adverse impact on the business. In devising a migration strategy, consideration must be given to the following points:

- Benefits of a 'phased approach' to migration.
- Options for out-of-hours working (evenings and weekends)

3.10. **Rectification Plans for Transition**

3.10.1. The Supplier will submit a "rectification plan" to the Council as per the following:

READ-ONLY

- The Supplier becomes aware that it will not achieve installation and testing of a service by the Service Commencement Date;

or

- The Supplier has failed to achieve installation and testing of a service by the Service Commencement Date, whether that failure arises because of:
  - The failure to deliver any or all deliverables prior to the service Commencement Date; or
  - The failure to successfully complete or achieve acceptance testing

3.10.2. A draft rectification plan shall be submitted to the Council no later than five (5) working days after the initial notification of failure or potential failure for agreement with the Council. The rectification plan shall identify the issues arising out of the delay and the steps that the Supplier proposes to take to achieve delivery in accordance with the agreement.

3.10.3. In case of emergency, the Supplier will immediately take all remedial action that is reasonable to avoid or reduce so far as possible such delay and the effects of such delay on achieving other Service Commencements and/or tests.

3.10.4. The approval and implementation of any rectification plan shall not relieve the Supplier of any responsibility to achieve Service Commencement and/or tests by their agreed date, or remedy any failure to do so, and no estoppel or waiver shall arise from any such approval and/or implementation.

3.11. **Delays Due to Contractor Default**

3.11.1. If a milestone is not achieved due to the Supplier's default (including where a deliverable does not achieve its associated acceptance test certificate so that the relevant milestone achievement cannot be completed by the agreed date), the Supplier shall in consultation with the Council promptly issue a non-compliance report to the Council. This non-conformance report shall;

- Categorise the test issues or, where no testing has taken place, shall set out in detail the non-conformities of the deliverables
- Include any other reasons for the relevant milestones not being achieved and set out the consequential impact on any other milestones

3.11.2. The Council may at its discretion (without waiving any rights in relation to the other options) choose to;

- Withhold any applicable milestone payment until the milestone is achieved with the issue of an acceptance test certificate.

3.11.3. The Supplier will be required to ensure that all costs associated with the installation, operation, service and service management are included within their submitted tender.

3.11.4. Suppliers shall be deemed to have satisfied themselves with the nature and extent of the requirement and obligations that are needed to meet the Council's requirements and the Council will not accept any claim as a result of any failure by the Supplier to seek clarification or undertake due diligence, or any liability for any claim or variation made on the grounds of insufficient knowledge of the nature or extent of the services required.

READ-ONLY

4. ICT SERVICE REPORTING AND SERVICE REVIEW

4.1. The Supplier will monitor the WAN, Internet Connectivity and Microsoft Express Route, in terms of (but not limited to):

(a) Initiate circuit maintenance and repair
(b) Timely monitoring of the network including:

a. Availability – including network port, access lines and Customer Premise Equipment (CPE) router as a %
b. Availability - Measured per site from the agreed "hub" site as a %
c. Latency – Round-trip delay measured in ms (milliseconds)
d. Packet Loss as a %
e. Jitter measured in ms (milliseconds)

(c) Remote Diagnostics and root cause analysis

a. Proactive Alarm Monitoring and Proactive Incident Management
b. Multi-channel customer notification service
c. Network services and CPE incidents
d. Threshold management - including confirmation as to how long a threshold must be exceeded before upgrades are recommended (Hours, Days, Weeks).
e. Bandwidth characteristics that aid the Council's innovation and flexibility

4.2. The Supplier will be required to confirm whether the transport network capacity is engineered for peak or average utilisations and must ensure that there is access to the network to enable the Council to perform the initial diagnostics on equipment placed within a Council location.

The Supplier shall:

(a) collate and format service performance statistics and supporting information in a format and frequency agreed with the Council;
(b) prepare and publish adequate and accurate service performance reports to demonstrate delivery against Service Levels for each ICT service identified;
(c) implement a web-based portal for the Council that shall enable all reports to be held and viewed electronically by appropriate Council personnel;
(d) provide digital dashboard presentation of information where appropriate;
(e) implement and operate a complaints register and escalation register with quarterly reporting;
(f) grant the Council or its agents the right to audit the service reports to determine if they represent a true and fair view of the Supplier's performance; and
(g) conform to the Council's report review requirements which may result in changes to the content, format and timing of such reports.

4.3. The primary interface for day-to-day service management shall be the Supplier's service desk, which shall monitor the performance against the agreed Service Levels and outputs and shall provide the Council with their specific ICT services reports.

4.4. Real time information – The Supplier's service desk personnel shall use the Supplier's system capabilities to monitor real-time Incident status information. The Supplier shall provide to the service desk personnel key metric information relating to the service performance.

4.5. The Supplier shall also implement a full infrastructure management solution based around an appropriate dashboard product set. This shall provide support staff with critical information

READ-ONLY

on the current service.

4.6. Services Report - The Supplier shall provide the Council on a quarterly basis a report outlining the performance of all areas of the service provided against the agreed Service Levels. The services reports shall be presented by the Supplier during the quarterly service review with the Council's managers. This is in addition to the online reporting that shall be available to the Council on a day-to-day basis. The appropriate members of the delivery areas shall be in attendance and available to explain any changes to the service. The services report shall cover performance against Key Performance Indicators and shall also report on key events such as projects and activities during the reporting period.

4.7. The format of the services report shall contain all the information as set out in this schedule and shall be finalised with the Council during the transition phase. Examples of the type of information contained in the report shall include but not be limited to:

(i) Complaints and major incidents;
(ii) First time fix rate.
(iii) Number outstanding incidents – by length and severity.
(iv) Number of service requests – implemented, waiting by implementation area.
(v) Continuous improvement – completed, planned.
(vi) Project status – RAG report on current projects.
(vii) Capacity management – reports on key capacity areas

The Supplier's service management response to be in line with the structure below:

- Severity 1: Emergency, major service disruption;
- Severity 2: High business impact, serious service disruption;
- Severity 3: Medium business impact, moderate disruption;
- Severity 4: Low business impact, minor loss of disruption

4.8. **Digital Dashboard**

4.8.1. On-line monitoring and reporting of the Council's ICT service shall also be performed by the integrated toolset. The toolset shall give centralised visibility and control of the Council's ICT estate.

4.8.2. The online tool shall provide the Council with customised data based upon permissions with extensive drill down capabilities.

4.9. **Escalation**

4.9.1. The Supplier shall maintain an escalation register. The initial point of escalation shall be via the service desk that shall then pass it on to the respective and appropriate Supplier personnel who shall act as the escalation channel for any issues relating to service delivery. If escalation is unable to resolve the service issues further escalation shall be made using the formal escalation process agreed with the Council.

4.10. **Audit**

4.10.1. The Supplier acknowledges and accepts the requirement of the Council for the right to audit the performance reports to determine that they reflect a true view on the service delivery in accordance with the agreement. The following responsibility matrix specifies in further detail the respective roles and responsibilities of each party.

READ-ONLY

Roles and Responsibilities	Supplier	Council
Service Reporting		
1. Define service level requirements and reporting cycles.		**X**
2. Document service-level objectives and requirements.	**X**	
4. Measure and analyse performance relative to requirements.	**X**	
5. Develop improvement and rectification plans.	**X**	
6. Authorise and approve improvement and rectification plans.		**X**
7. Implement improvement and rectification plan.	**X**	
8. Report service-level results.	**X**	
9. Coordinate monitoring and reporting with the service desk.	**X**	
10. Provide appropriate metrics and measures of performance to appropriate Council representatives.	**X**	

4.11. **Transition**

4.11.1. The Council and Supplier shall work together to achieve the transition activities and 'to be' outcomes outlined below in accordance with the Agreement and relevant schedules.

The Supplier shall:

Transition	Transition Outcomes
(a) Identify and understand the current ICT service reports. (b) Agree the metrics and measures that shall form part of the service reporting solution. (c) Agree the format, content and frequency of the service reports. (d) Review existing processes and inputs to service reporting. (e) Agree the digital dashboard requirements.	(a) Develop complaints management processes with the Council to improve resolution rate and improve service delivery. (b) Develop and implement the dashboards to support service reporting. (c) Ensure that the Council can audit the performance reports.

4.12. **Detailed Requirements**

Quarterly Service Reviews

Each quarter the Supplier shall carry out a service review of the services which shall include but not be limited to:

4.12.1.1. establish whether the Supplier is providing the services in accordance with Schedule 2.2 (Standards and Service Levels) and other requirements of this Agreement;

4.12.1.2. assess the Supplier's performance of the services as against the KPIs and other PIs; and

4.12.1.3. the review shall meet the objectives stated in this schedule and shall be carried out on the basis of the detailed requirements of this ICT services reporting and service review section.

4.12.1.4. the Supplier shall submit to the Council within agreed timescales a comprehensive and detailed written ICT service report carried out in accordance with this schedule and the main agreement, such reports to be based on a service review and to contain:

(a) a status report of the progress of any projects being undertaken by the Supplier;

READ-ONLY

(b) the results of the measurement of the Supplier's performance of the services including:
(i) system/network availability;
(ii) service desk incidents analysis including by priority, and type;
(iii) service desk performance;
(iv) performance against KPIs within Schedule 2.2 (Standards and Service Levels);
(v) security report;
(vi) infrastructure performance and capacity report
(vii) service requests analysis;
(viii) financial/costing/billing analysis;
(ix) Council satisfaction;
(x) asset register;
(xi) complaints register;
(xii) register of changes under change control procedure;
(xiii) service improvement plan
(xiv) where relevant, any further significant issues surrounding service performance which are not covered by the matters referred to in section 2 above and ways in which such issues have been addressed;
(xv) any other matters reasonably requested by the Council; and
(xvi) the Supplier's proposal for implementing the outcome of its review including the action which the Supplier proposes to take in order to improve its performance in the areas for improvement identified together with the timescales for taking that action and relevant information to enable the Council to assess the actions identified as necessary in previous service reviews.

4.12.2. The Supplier shall ensure that each report clearly shows the results of the KPIs for the immediately preceding thirteen (13) service reviews such that the Council can evaluate the quarterly performance trend.

4.12.3. **Annual service reviews**

4.12.3.1. Prior to and after each review date the Supplier shall carry out a review of the provision of the services by or on behalf of the Supplier in the year up to the review date (including a review of the performance of relevant parts of the Supplier's organisation carrying out the services and any Sub-Suppliers). Such review shall take account of the relevant service development plan and compare the objectives in the service development plan with the actual provision of the services.

4.12.3.2. No later than twenty (20) Working Days after the relevant review date the Supplier shall submit to the Council a comprehensive written report of the outcome of the annual service review, such report to contain:

(a) an explanation of the process undertaken by the Supplier in carrying out the review;
(b) results of the review of performance against KPIs and PIs and against the requirements of Schedule 2.2 (Standards and Service Levels) and the service credit regime and generally, including an analysis of trends and reasons for trends;
(c) set out a detailed and transparent tracking of any proposed incremental improvements and any other changes to the Service Levels, against each relevant area of Schedule 2.2 (Standards and Service Levels) which is being supplemented, varied or replaced;
(d) a status report on progress of any projects undertaken by the Supplier and details of work undertaken by the Supplier in relation to proposals for projects in that year such information shall also be set out in the service development plan; and
(e) set out the action which the Supplier proposes to take in order to improve its performance in the areas for improvement identified by the review together with the

READ-ONLY

timescales for taking that action.

4.13. **Outcome of Service Reviews**

4.13.1. If the Council is satisfied with the quarterly and/or annual service report issued by the Supplier, the Supplier shall forthwith implement the proposals set out in the service report (including any actions which have been identified) in accordance with the timescales set out in the report. If the Council is not satisfied with the service report, the Council shall (acting reasonably) suggest amendments or clarifications and provided they are reasonable, the Supplier shall make such amendment or provide such clarification of the quarterly and/or annual service report as reasonably requested by the Council within ten (10) Working Days of the request by the Council or such other period agreed between the parties.

4.13.2. The following provision applies to the conduct of annual service reviews. Upon acceptance of the report, the Supplier shall (if applicable and agreed) vary the Service Levels as set out in the report with effect from the date of acceptance of a Change raised in accordance with the Change Control Procedure.

4.13.3. In no circumstances shall the Service Levels or KPIs deteriorate or diminish as a result of the annual service review. If the Council does not accept the outcome and proposals set out in the Supplier's report this agreement shall continue in full force and effect and neither the Service Levels, KPIs or any other provision of this Agreement shall change or be deemed to have changed as a result.

READ-ONLY

5. SERVICE AND SERVICE DESK MANAGEMENT

The Supplier shall:

(a) provide a service desk that aligns to the ITIL framework and guidelines for all the ICT services which shall manage all service and support requests through multiple communications channels including but not limited to phone, email and web portal, covering (but not limited to) change, incidents and requests The service desk shall be the primary point of Council contact with the Supplier for incident reporting, problem management and resolution, change requests, service extensions and ad-hoc requests; and provide reasonable advice, information and guidance on all service related matters. The service desk shall be available at the times specified with each level of service required and shall have a designated single telephone number and shall use a single designated email address and have an associated self-service web portal with the ability to track the progress of incidents and requests;

(b) provide the ability to log calls outside the core service desk hours;

(c) allow for all calls to be logged/registered onto the Supplier's service desk;

(d) prioritise and resolve each call according to the severity of incident in accordance with the Service Levels;

(e) ensure the service desk shall co-ordinate fault resolution and incident management for all incidents and enquiries relating to the services through the service desk including those relating to third party suppliers;

(f) provide first line support to the Council so that operational incidents and queries are resolved as quickly as possible;

(g) provide and manage an asset management service (including an asset register) for all Configuration Items and ensure that a comprehensive and accurate asset register is maintained at all times and a knowledge base is built up about assets and any related incidents. Access to the asset register shall be provided to nominated Council staff; and

(h) resolve support calls in line with the requirements of Schedule 2.2 (Standards and Service Levels).

(i) implement, deliver and maintain a Council care policy to support the users. The policy shall ensure that the Supplier complies with all of the requirements relating to the service desk and that in particular:

  (i) service desk staff respond to users in a professional and courteous manner;

  (ii) service desk staff follow up complaints and enquiries; and

  (iii) the Supplier takes ownership of and responsibility for all support calls until the call is resolved.

(j) use appropriate management systems and tools to enable support calls to be logged, tracked, analysed and escalated;

(k) use appropriate management systems to promote user knowledge and competency including answers to frequently asked questions;

(l) provide a web-based system which shall allow a user to log and track all support calls logged on a 24x7 basis irrespective of the method the support call was originally communicated to the service desk. Appropriate access, including report generation, to Council service management records to be provided for up to 8 Council authorised users;

(m) notify key Council staff of call resolutions and closure for all severity 1 and 2 incidents via email;

(n) develop appropriate Operational Level Agreements with all third-party suppliers and Council internal teams with agreed responsibilities in relation to the resolution of particular service issues.

5.1. Service desk staff shall assign a severity level with the Council to the agreed severity level

READ-ONLY

definitions and standards. The service desk staff shall gather and record as much information as necessary concerning the incident and attempt an initial resolution at the first point of contact.

5.2. Where this is not possible then the call shall be passed to the agreed resolver group. These incidents shall then be tracked and progressed until closure. When incidents are likely to exceed their agreed performance levels then the service desk staff shall escalate the incidents as per the escalation process.

5.3. The service desk shall generate statistics and shall produce reports in the agreed format as part of the agreed service monitoring arrangements and including:

- Management Network (WAN) – across all layers
- Internet Connectivity
- Microsoft Express Route

5.4. All service desk agents shall have access to system management tools to enable them to remotely diagnose, manage and resolve incidents and access both internal and external knowledge repositories.

5.5. The toolset that is used by the service desk agents shall also record all asset information and populate the system with the information related to the user and their associated assets. The following responsibility matrix specifies in further detail the respective roles and responsibilities of each party:

Roles and Responsibilities Matrix	**Supplier**	**Council**
General		
1. Monitor and manage incidents until successful incident resolution	**X**	
2. Communicate any temporary changes to Service Levels or service degradation and any relevant scheduled maintenance information.	**X**	
3. Define policies and procedures		**X**
4. Ensure that root cause analysis is performed and reported on all recurring incidents	**X**	
Planning & Analysis		
1. Perform service desk capacity monitoring and planning	**X**	
2. Perform service desk staffing analysis to ensure service desk is staffed with personnel having the appropriate sets of skills, training, and experience in line with Council capacity and technology	**X**	
Operations & Administration		
1. Staff and maintain a service desk as per the Council's requirements	**X**	
2. Monitor and respond to service requests submitted via email and other communication channels	**X**	
3. First point of contact for all problem determination and resolution.	**X**	

READ-ONLY

4. Categorise and log ICT information requests incidents/problems/service requests in accordance with agreed processes and standards	X	
5. Resolve incident/problem request/service resolution requirements	X	
6. Restore and/or resolve inquiry/problem within prescribed time limits, if possible, otherwise escalate to appropriate Level	X	
7. Identify problem characteristics and, wherever possible, root cause analysis in order to create a knowledge management repository	X	
8. Notify the Council and vendor management as required	X	
9. Monitor and manage problems until successful problem resolution	X	
Root Cause Analysis		
1. Flag all Severity Level 1 and Severity Level 2 Incidents as requiring root cause analysis	X	
2. Ensure that appropriate resources within the Supplier are assigned as may be necessary to identify and remedy the failure, and track and report any consequences of the failure	X	
3. Identify root cause of Severity 1 and Severity 2 level problems or failures and recommend appropriate resolution action, where/whenever possible	X	
4. Track and report on progress of all Severity 1 and Severity 2 level problems that are escalated to Level 2 support to ensure that root cause analysis performed and reported on (incident reports / tickets to remain open until root cause analysis report is completed and submitted)	X	
5. Provide the Council with a written report detailing the cause of and procedure for correcting such failure; provide updates on a quarterly basis until closure	X	
6. Substantiate to the Council that all reasonable actions have been taken to prevent recurrence of such failure	X	
7. Review and approve actions for resolution of problems as reported in root cause analysis recommendations		X
Asset Management		
1. Manage/track service orders	X	
2. Coordinate delivery and installation of new products and services	X	
3. Ensure compliance with established Council ICT standards and architectures	X	
4. Adhere to Council acceptance process	X	
Monitoring & Reporting		

READ-ONLY

1. Define service desk SLA		**X**
2. Document service-level objectives and agreements	**X**	
3. Measure and analyze performance relative to objectives and agreements	**X**	
4. Develop improvement plans where appropriate	**X**	
5. Authorise improvement plans where appropriate		**X**
6. Implement improvement plans	**X**	
7. Report service-level results	**X**	
8. Report service desk statistics and trends as requested	**X**	
9. Audit results & operations periodically		**X**

5.6. INCIDENT AND PROBLEM MANAGEMENT

5.6.1. The Supplier shall:

(a) monitor all open incidents and must escalate unresolved incidents, in accordance with the agreed escalation procedures when Service Levels are not achieved;

(b) provide a call closure procedure to be agreed by the Council whereby after an incident has been resolved and the Council has been informed, there is the opportunity for the Council either to agree to the call closure or to disagree;

(c) proactively monitor incident trends to identify where multiple incidents have the same symptoms and resolution. These incidents are to be classified as a 'Problem' and given a unique problem reference number. All Problems shall be recorded in an electronic problem log which is to be made available to the service desk and Council Identified Problems should be converted into Known Errors and a permanent resolution or workaround developed within the period defined in the SLA. A permanent resolution must be provided unless it can be demonstrated to the reasonable satisfaction of the Council that no permanent resolution is available for the Problem.

If a third-party supplier becomes involved in resolving a support call, then the service desk, acting in agreement and in conjunction with the local application administrator shall:

(d) manage and liaise with the third party to resolve the incident and leave the call open until resolved;

(e) obtain from the third-party supplier details of the actions taken by and ensure that any details provided are updated to the appropriate records maintained by the Supplier;

(f) be responsible for liaising with the third party supplier to obtain progress information on a regular basis consistent with the priority of the incident and the agreed Service Levels; and shall (where the relevant support contract is between the Council and the third party) act as the technical contact on behalf of the Council;

(g) follow the agreed major incident process as defined in the Operations Manual; and

(h) use reasonable endeavours to verify that all incidents assigned to third parties are resolved within the agreed time as specified in the relevant Managed Supplier Contract Service Levels.

(i) resolve all incidents assigned to CGI resolvers in line with the Service Levels defined in Schedule 2.2 (Standards and Service Levels).

5.6.2. All incidents shall be recorded on the Supplier's management system, together with an agreed priority (severity), applicable Service Levels and escalation agreements. These shall be able to be monitored by users via the self-service portal.

READ-ONLY

5.6.3. The Supplier shall gather and record as much information as necessary concerning the fault and attempt an initial resolution at the first point of contact. Where this is not possible then the call shall be passed to the agreed resolver group. These incidents shall then be tracked and progressed until closure. Where incidents are likely to exceed their agreed performance levels then the service desk staff shall escalate the incidents as per the escalation process. When it is believed that an incident is resolved then the service desk shall contact the end user using the appropriate contact method as determined by the Council (if available) and ensure that it is fixed to his/her satisfaction and shall then close the incident otherwise it shall be placed in a pending state awaiting user feedback. If the user does not respond within ten Working Days, then the call shall be auto-closed. Where the user reports that the incident is not resolved the incident shall be returned to the relevant party for further investigation.

5.6.4. The Supplier's problem management function within the service desk shall proactively monitor incidents using its ITIL aligned problem management processes.

5.6.5. Where an incident occurs in relation to suspected or actual security breach, the Supplier shall inform the Council and assist the Council as appropriate in managing the incident in accordance with Council Security Incident Process and the agreed ISMS.

5.6.6. Where trends and repeat incidents are identified a problem record shall be created and all relevant incidents shall be assigned to the problem. A resolution or workaround to these problems shall be formulated and may require the assistance of different resolver groups, technical resources, third parties or the Council. The liaison and management of the differing resources shall be owned and managed by the Supplier's problem managers. Once a resolution or workaround has been established it is the responsibility of the problem manager to obtain the information from the relevant parties, formulate a formal response and discuss this with the Council.

5.6.7. All problems shall be entered into the known errors database and a workaround or permanent resolution shall be established within twenty (20) Working Days or as agreed between the parties. The Supplier shall generate statistics and shall produce a report in the agreed format as part of the service monitoring arrangements.

5.6.8. All service desk agents shall have access to system management tools to enable them to remotely diagnose, manage and resolve incidents and access both internal and external knowledge repositories. End users shall be able to access frequently asked questions held on these knowledge repositories.

5.6.9. The Council shall:

(a) provide input from the service prior to the services commencement date into establishing the new service;
(b) assist in the knowledge transfer to the Supplier from the Council;
(c) provide relevant local business skills and expertise to assist the Supplier in problem resolution;
(d) make available all relevant third-party agreements; and
(e) appoint the Supplier as managing agent (or similar) to enable the Supplier to place calls with third party suppliers on behalf of the Council.

READ-ONLY

6. CONFIGURATION AND CHANGE MANAGEMENT

6.1. Requests for change must be triggered for any one-off, but not limited to, the following events:

- A new resolution for an incident or problem
- A proposed upgrade to some component of the infrastructure
- Changed business requirements or direction
- Location changes

6.2. The Supplier shall:

(a) be responsible for managing, maintaining and documenting the configuration of the WAN infrastructure;

(b) the configuration documentation shall be accurate and complete and shall contain up-to-date information, including historical changes and source information, to a level of detail needed to maintain and manage the Infrastructure. Where updates need to be made these shall be agreed and signed off by the Council's client manager;

(c) implement, change, upgrade and undertake release management in line with ITIL and ISO/IEC 20000 standards;

(d) prepare release plans to be discussed during quarterly reviews, or sooner if appropriate, for all non-incident-based upgrades as agreed by the Council and which are to be treated as either scheduled maintenance or as an emergency release as part of an incident resolution;

(e) liaise with the Council to agree scheduled outages as described in the scheduled maintenance plan, which plan shall be agreed between the Council and the Supplier on an annual and quarterly basis;

(f) maintain, on behalf of the Council, the current production versions of images in a fully comprehensive asset register;

(g) maintain an asset register on behalf of the Council with the accuracy as defined in the SLA as measured on a quarterly basis. The Supplier will be required to manage and record accurate and up to information data on the assets deployed within the Council's locations, including (but not limited to):

- Site location including postal address
- Manufacturer, Model number and Model Version
- Manufacturer serial number
- Management IP address
- Physical connections
- Installation / refresh date

and

(h) ensure that there is only be one instance of the asset register.

6.3. Configuration Management

6.3.1. Configuration management and the configuration management database ("CMDB") shall be at the heart of the Supplier's service management toolset. Good quality inventory management information shall form the foundation on which the Supplier's configuration management process is built. The inventory register shall act as the 'single source of accuracy' containing the information relating to the managed components within the Council's ICT estate.

6.3.2. The Supplier's service management tool shall hold the Council's inventory list; the

READ-ONLY

information held in the inventory list shall be a combination of automatically gathered technical attributes and manually managed information such as owners and locations. Inventory information shall form an integral component of the overall CMDB.

6.3.3. The CMDB shall hold a comprehensive range of information that can be related to any item in the Council's inventory list. Listed below are the main inventory sections of the Supplier's CMDB and a short description of the information that is held within them.

6.4. Location and Categorisation

6.4.1. Every item in the inventory list shall be tagged with a non-branded asst sticker using a consistent format that is used throughout the system. Categorisation shall ensure that other system modules e.g. change management, can effectively search and relate to configuration items ("CIs"). The system shall also track both the physical and business location of equipment.

6.5. Configuration Item (CI) Audit

6.5.1. The system shall maintain full version control and an audit trail of every data field within a CI record.

6.6. External Attributes

6.6.1. Where applicable the Supplier's system shall maintain URL links to management tools that hold additional information relating to an individual CI.

6.7. Additional Attributes

6.7.1. To ensure complete flexibility in terms of the information that is held in the CMDB each categorisation of CI, (e.g. routers) shall have a specific attribute set applied to them. This enables the system to hold detailed attribute information for specific types of equipment within a single centralised CMDB.

6.8. Documentation

6.8.1. Wherever a change to a CI is required, in order to minimise the risk to the Council, the Supplier's change management processes and procedures shall apply.

6.9. Change Management

6.9.1. A change management function shall be provided by the Supplier as part of the core service provided to the Council. This service shall be provided in line with the agreed change policy through a forward schedule of change ("FSC") and ITIL process.

6.9.2. The change management function shall ensure that standard and major changes are assessed and implemented in such a way as to minimise the risk of an adverse impact on service. Change management shall also ensure that the benefits of a change are balanced against the costs (financial, reputational, institutional or opportunity) and risks associated with the implementation of the change.

6.9.3. The Supplier shall utilise an appropriate method to document and manage change, which shall provide a full audit trail. Change management shall manage change activities and provide input to the CMDB control process.

READ-ONLY

6.9.4. The Supplier shall:

(a) Implement change management across all areas supported by the Supplier in the Council
(b) Integrate the change management output with standard reporting mechanisms to the Council.
(c) Ensure that the release management process is used as required.

6.9.5. Within the change management service, the Supplier shall review, categorise and assess requests for change ("RFC"), communicating with the impacted Council's business and/or the Supplier departments where necessary before authorising the RFC.

6.9.6. If the Supplier believes that the RFC shall have a detrimental effect on the infrastructure, then it shall recommend to the CAB that the change be rejected or modified. The FSC and performance of the change, release and configuration, regression planning shall also be discussed in the quarterly service review meetings.

6.9.7. Where numerous Configuration Items (CI's) are affected by a change (e.g. a new system roll-out or large-scale patch), the release process may be triggered (the metrics used for triggering the release management process shall be agreed beforehand in the release policy).

READ-ONLY

7. ICT PROCUREMENT SERVICE

7.1. The Supplier is required to ensure that there are effective procurement processes with regards to how the Council would procure any future/additional services that align to the WAN solution. This includes, but is not limited to:

- tender and pre-acquisition advice from the Supplier in accordance with the Council financial regulations
- Ordering, staging and delivery of service from the Supplier
- Delivery, installation and service transition from the Supplier
- Returns and order verification from the Supplier

7.2. For clarification, the Council is expecting any future/additional services to be:

- Included and managed under the agreed WAN contract
- Included in the account management review meetings
- Included in the SLA / Service Management

7.3. Where a change is requested, and no pricing is contained within the agreement or can be established based on an existing service, the Supplier shall be responsible for the provision of a quotation for the cost of the change, which shall;

- Be based on and reflect the principles of the pricing provided for within the Suppliers' tender
- Include (if applicable) estimated volumes of each type of resource to be employed, the experience of each resource (if applicable) and the cost of each type of resource.
- Include full disclosure of any assumptions underlying the quotation
- Include evidence of the cost of any assets required for the change

7.4. The Supplier shall:

(a) ensure any agreed technology refresh program is compliant with the agreed strategic and technical direction of the Council;
(b) pass onto the Council, on an open book, auditable and justifiable basis, any volume discount obtained by the Supplier, subject to the terms of such volume discount agreement;
(c) provide professional and technical advice in the procurement of major new systems, from development of the specification of requirements (including the development of outline and full business cases) through to post-implementation review or in any tender exercises;
(d) run regular vendor and cost/price comparison benchmarking reviews and ensure the Council obtains competitive pricing for the purchase of its ICT assets/services;
(e) Pro-active bench marking activities to ensure best value is offered, taking account of cost and Service Levels.
(f) Continuous review of products on the market and recommendation of alternatives offering better value. This to include an evaluation service for new lines, models.
(g) Regular reviews to discuss the latest ICT developments within the ICT industry.
(h) Regular reporting on agreed parameters as defined by the Council and in accordance with agreed timeframes.
(i) If the request is for a quotation, the local procurement team shall obtain pricing within the SLA and shall update the call with the price and e-mail the quote to the requestor.
(j) If the request is for goods to be ordered, then an order shall not be placed until an authorised purchase requisition or order is received from the user. The call shall then be updated with the order details and delivery date and is assigned to the relevant support team, depending on the item being procured.

READ-ONLY

8. CAPACITY PLANNING/PERFORMANCE MONITORING

8.1. The Supplier shall:

(a) proactively provide capacity planning and performance monitoring on all network components and identify/propose plans to alleviate any potential capacity or performance pressure points;
(b) monitor, and collect capacity statistics and report on an exception basis including but not limited to network utilization
(c) provide a quarterly analysis to the Council for all network hardware, including but not limited to performance, capacity, and utilisation. Include forecasts and any recommendations for amendments/upgrades to the infrastructure; and
(d) provide work plans to the Council (at least one month in advance of the work commencing) to address potential risks to the performance of the infrastructure. The plan should be presented to the Council with sufficient time to allow the proposed work to be agreed, coordinated, resourced and carried out in advance of any impact to the Council's business operations.

8.2. **Infrastructure Performance Monitoring**

8.2.1. The Supplier shall operate an infrastructure performance monitoring service that monitors, captures and analyses real time information (where appropriate and technically feasible) from the hardware and software used to deliver the ICT services to the Council.

8.3. **Capacity Planning**

8.3.1. The services provided to the Council shall include a combination of people, process and tools to provide a comprehensive capacity planning service. The service shall take into account resource, service and business planning (in conjunction with the Council) to provide a comprehensive service.

8.3.2. Infrastructure reporting. The performance information generated by the above tools shall be stored centrally and collated to form the basis for infrastructure capacity planning. The data shall be analysed on a regular basis and provide input to the quarterly service review meeting. The report shall include Network hardware utilization and Network link utilization.

8.3.3. The Supplier and the Council shall define the detailed content of the report during the transition phase.

The Supplier shall:

(a) Produce work plans in line with the Council's business planning cycle, identifying capacity requirements early enough to take account of procurement lead times and the Council's approval processes
(b) Report and plan the need for any increase or reduction in hardware based on Service Levels and cost constraints.
(c) Assess new technology and its relevance to the Council in terms of performance benefits and cost.
(d) Assess new hardware and software products for use by capacity management that shall improve the efficiency and effectiveness of the process.
(e) Carry out performance testing of new systems.
(f) Report performance against targets.
(g) Recommend tuning of systems and make recommendations to the Council on the design and use of systems to help ensure optimum use of all hardware and operating system software resources.

READ-ONLY

(h) Recommend resolutions to performance-related incidents and problems
(i) Carry out ad-hoc performance and capacity studies on request from the Council.
(j) Carry out or, participate in, risk reviews of potential changes and business plans to minimise the risk of all changes.

8.3.4. A primary output from the Supplier's capacity planning process shall be a formal "capacity plan" a living document that shall reflect ICT infrastructure plans in the context of the Council's business and Education service plans. This plan shall be reviewed and revised annually.

9. INFRASTRUCTURE MAINTENANCE

9.1. For any scheduled Supplier maintenance activities that could adversely affect the Council services, the Supplier shall provide the Council with at least thirty working days advance written notice of the maintenance activity and obtain the Council's sign-off on each batch of activity.

9.2. The Supplier is to confirm the maintenance release schedule for all devices, software, firmware and other service provided under the contract agreement.

9.3. The Supplier shall:

(a) manage the process of scheduling maintenance in accordance with agreed release management procedures. Scheduled maintenance shall be any activity which can be scheduled, and is necessary, and which if not carried out would have an adverse impact on the achievement of the Service Levels;
(b) carry out emergency maintenance during the allocated scheduled maintenance hours where it is agreed with the Council. There shall be no scheduled outages of the network during business hours unless otherwise agreed by the Council and Supplier;
(c) where appropriate, ensure that automated tools are used to deploy scheduled maintenance services;
(d) ensure scheduled maintenance is not carried out to the exclusion or detriment of any of the other services.

9.4. For any scheduled maintenance activities that could adversely affect the Council services, the Supplier shall provide the Council with at least thirty working days advance written notice of the maintenance activity and obtain the Council's sign-off on each batch of activity.

9.5. Emergency maintenance shall be subject to the predefined emergency change policy and applied and documented as appropriate but shall still require agreement from the Council before it is performed.

READ-ONLY

10. SECURITY MANAGEMENT

10.1. **Network Security** - The Supplier will need to ensure their standard security operation procedures (SOP) for the Council's WAN solution is secure in terms of;

- Data when traversing the WAN solution is secured away from other customer's data or internal divisions
- Data when traversing the WAN solution is secured away from unauthorised utilising of the same network
- Data is secured in the event of internal and external intrusion
- The procedure of informing the customer as to any attempted violations
- Evidence that the Supplier has a current ISO 27001 compliance certification. The Supplier will be required to maintain the compliance with ISO 27001 during the term of the contract.

10.2. **Trap and Trace** - The Supplier must provide timely and effective assistance to the Council when the Council is experiencing a network attack that is utilising the WAN, Internet service or Microsoft Express Route connection, or any part of the Supplier's wider network as a means of delivery / access. This includes, but not limited to, the following attacks:

- Denial of Service (DOS) and Directed DOS (e.g. service and reports)
- IP spoofing (e.g. service and reports)
- Illegal and/or Council policy-defined unacceptable use of Council's ISP connection (e.g. service and reports)
- The procedure of informing the customer as to any instances of attempted violations (e.g. process and reports)

10.3. **Indirect / Unauthorised Access -** The Council will not accept connection on to the WAN from a third party unless authorised by the Council. The Supplier must ensure that their solution does not contain any means of connectivity on to the WAN without authorisation.

10.4. **Security Performance Monitoring -** The Supplier will provide timely and effective assistance (including, but not limited to access to data, services and the appropriately skilled / experienced personnel) to the Council in order to;

- Identify, prevent and mitigate any security breaches
- Identify, prevent and mitigate any malicious attacks

10.5. **Physical Security –** The Supplier will be required to provide an effective layered approach to physical security that covers the Council's firewalls located within their data centre or within their designated third-party Internet Breakout point. The Supplier will be required to ensure that there is:

- Location and Site security
- Security zones
- Detection and monitoring systems to deter, detect and delay any attacker

10.6. **Express Route via Exchange Provider** – If the Microsoft Express Route is being provided via the Exchange Provider option, then the Supplier is required to provide:

- The security and network architecture for the design
- Any 3rd parties involved in the design
- Any SPOF's within the design

READ-ONLY

- The security considerations undertaken due to the Exchange Provider option being proposed ensuring that the security requirements are met

10.7. **Root Cause Analysis** – Following the Council experiencing an issue with any of the above Security items, the Supplier will assist in a timely and effective manner (including, but not limited to access to data, services and the appropriately skilled / experienced personnel) the Council identifying the root cause of the security breach.

10.8. The Supplier shall:

(a) manage all technical security aspects of the in-scope systems and infrastructure and implement appropriate measures to ensure that the infrastructure is protected from deliberate or accidental breach of security, and preventing unauthorised access;
(b) take appropriate steps in accordance with agreed policy and process to ensure the security architecture protects the Council from the latest security attacks and threats and notify the Council immediately of any potential major risk/threat to the Council's network e.g. impending virus attack;
(c) provide a service that embraces the principles and working practices as defined in ISO/IEC 117799 /BS27001 and any revision or updates to this standard, with the aim of ensuring the confidentiality, integrity and availability of in-scope Council data;
(d) provide all necessary guidance to the Council on detecting and preventing security incidents and provide such information as is necessary for the Council to comply with its statutory and business requirements such as PSN and PSBA and PCI compliance;
(e) provide internal network security and access controls in conjunction with the Council and other suppliers, and in accordance with agreed process and responsibilities, Council polices and recognised industry standards and the Council's specific requirements;
(f) technically enforce and manage in scope systems security with immediate notification to the Council of potential incidents, suspected or identified systems security breaches in accordance with the agreed ISMS;
(g) enforce and manage appropriate in scope systems security and protection policies across all Council systems/assets and infrastructure
(h) notify the Council within 60 minutes (or such other period as may be agreed in relation to particular types of incidents) of detection of any incidents of suspected, attempted or actual misuse of, or security incidents affecting the infrastructure, including any deliberate attempts of which it is aware to gain unauthorised access to any component of the infrastructure.

10.9. The Supplier will not make or allow to be made any changes to the services which may affect the performance (including functioning, implementation and operation), security or PSN compliance of the services.

Roles & responsibilities	**Supplier**	**Council**
Security Management Service		
Develop security policies and procedures that comply with the Council's security requirements.	**X**	**X**
Implement and maintain security methodologies, practices, and monitoring processes that are in compliance with approved policies and procedures.	**X**	
Maintain physical security of facilities, networks, systems, data and assets.	**X**	**X**
Maintain logical security of facilities, networks, systems, data, and assets.	**X**	
Conduct periodic security checks per requirements, document results of checks in security reports, and provide reports to the Council.	**X**	

READ-ONLY

Monitor security and investigate and report security violations and breaches.	**X**	**X**
Resolve security violations and breaches that are determined to be within Supplier's controlled environment parameters, liaise with the Council as appropriate and report actions taken to avoid recurrence.	**X**	
Resolve security violations and breaches that are determined to be within Council controlled environment parameters with the assistance of the Supplier as appropriate.		**X**

READ-ONLY

11. FUTURE PROJECT CONSIDERATIONS – SERVICE DEVELOPMENT

11.1. **Service Improvements –** The Supplier will be expected to demonstrate their ongoing obligation to the Council throughout the Contract Period to identify new or potential improvements to the Services pursuant to which it will regularly review with the Customer the Services and the manner in which it is providing the Services with a view to reducing the Customer's costs (including the Contract Charges) and/or improving the quality and efficiency of the Services.

11.2. To achieve increased efficiencies, financial and technological benefits, the Council is looking to embrace a change in connectivity technologies. The WAN, Internet connectivity and Microsoft Express Route, in the future will be characterised by:

- Technically scalable in order to meet the businesses future demand;
- Flexible service provision to reflect the Council's development and consumption of services, irrespective of hosting;
- Increased functionality in terms of quality and class of service provision, support for greater use of technology and on-demand service provision;
- A range of support service offerings that directly reflects the business requirements;
- A more financially sustainable approach to the provision of connectivity across the Council;
- Enable reduced reliance on any single BCP building;
- Enable user mobility;
- Increase efficiency whilst significantly reducing costs

11.3. The Supplier shall therefore commit to the process of continuous improvement and improved efficiency of the services throughout the term of the contract. The Supplier will therefore take the initiative in identifying and evaluating improvements for application to the services to the Council and responding to any Council requests for information in respect of potential improvements to the services that the Supplier has identified. As part of this obligation, the Supplier shall identify and report to the Council, on a six-month cycle (or earlier if appropriate);

- The emergence of new and evolving relevant technologies which could improve the services and those technological advances potentially available to the Supplier and the Council which the parties may wish to adopt;
- The potential improvement to the service including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and Council support services in relation to the services;
- The potential improvements to the interface or integration of the services with the other services provided by third parties or the Council which might result in efficiency or productivity gains or in reduction of operational risk;
- Any changes in the business processes and ways of working that would enable the services to be delivered at lower costs and/or greater benefits to the Council.

11.4. The Supplier will ensure that the information that it provides to the Council shall be sufficient for the Council to decide whether any improvement should be implemented. The Supplier shall provide any further information that the Council reasonably requests.

11.5. **Innovation and Continuous Improvement**

11.5.1. The Council expects the Supplier to use technology and innovative approaches to improve the management and efficiency of the WAN, Internet Connectivity and Microsoft Express Route so ensuring the most cost-effective Total Cost of Ownership (TCO).The Council requires the Supplier to have an ongoing obligation throughout the Contract Period to identify new or potential improvements to the Services pursuant to which it will regularly review with

READ-ONLY

the Customer the Services and the manner in which it is providing the Services with a view to reducing the Customer's costs (including the Contract Charges) and/or improving the quality and efficiency of the Services.

11.5.2. **Contract Flexibility** - the Council requires the Supplier to ensure that there is a level of "flexibility" in the delivery of the services including the reduction and / or growth in number of sites and services the Council consumes during the period of the contract.

11.5.3. The Supplier shall:

(a) provide project management services, as required and requested by the Council. The details of the project management services to be provided shall be agreed by the parties on an individual project basis;
(b) ensure that any project management service provided uses the main elements of the PRINCE2™ methodology (e.g. project initiation, project planning, progress reporting, risk management, project organisation, project documentation management project closure and post implementation reviews) The Supplier shall conform to the Council's requirements in respect of project gateway reviews unless agreed by the Council to the contrary; The Supplier shall conform to changes required to project methodologies as a result of the project management reviews, changes to industry best practice or Council requirements;
(c) provide, maintain and make available to the Council all project documentation, including management, specialist and quality documentation associated with the project and provide the Council with a perpetual license to use and distribute such documentation;
(d) ensure that sufficient and adequate communication shall take place between the Supplier's project management staff and the Suppliers service management staff and where appropriate Council staff to ensure that all aspects of project handover and exit are handled efficiently;
(e) provide project progress information, by an online project portal in addition to individual progress reports as required by the Council in hard or soft copy format; and
(f) ensure that any programme management provided uses the main elements of the "Managing Successful Programmes" (MSP®) methodology unless agreed by the parties to the contrary.

11.5.4. The Supplier shall provide project and program management services as requested by the Council. The Supplier shall seek to understand current operations, and then agree a framework within which to deliver project services, based upon the main elements of the MSP® and PRINCE2™ methodologies.

11.5.5. The overall aim of the service is to provide a project management service that shall ensure all project work is managed effectively; that is on time, to budget, quality and specification, whilst also allowing the Council to realise the benefits defined within the business case.

11.5.6. The Supplier can deploy its program and project management resources for the Council to either lead or support the Council's in-house teams or take responsibility for managing complete projects and work streams.

11.5.7. The Supplier shall provide continuity of project resources to the Council by assigning a core project team for each individual project engagement, with the necessary project management skills and the required technical skills. Specialist and additional resources shall be added if required by a particular project or projects. The skill levels and experience required for any particular project shall be taken into account by the Supplier before assignment, or in the case of a project manager new to the Council, before that project manager is proposed.

11.5.8. Once individual Supplier staff have been assigned to a Council project, the Supplier shall provide continuity of these personnel for the duration of the project engagement.

READ-ONLY

11.5.9. The Supplier shall agree with the Council a flexible commercial model for the delivery of project and program services; designed to ensure that the Council receives value for money and only pays for project services that have been used. The Council shall: hand over or procure the handover of the documentation for any projects that are underway that shall transfer to the Supplier on the Commencement Date.

11.5.10. The following responsibility matrix specifies in further detail the respective roles and responsibilities of each party.

Roles and Responsibilities	**Supplier**	**Council**
Project Management Services		
1. Provide project managements services in support of the Council's strategic development plan.	**x**	
2. Attend individual project board meetings for projects as required by the project board.	**x**	
3. Attend the Council's corporate project planning meetings on a quarterly basis or as otherwise required up to maximum number of 6 per annum.	**x**	
4. Take responsibility for managing individual projects within the framework of the PRINCE2™ project management methodology as required by the Council utilising all the key attributes of the methodology as appropriate to the size and complexity of the project and including the development and maintenance of appropriate project documentation.	**x**	
5. Approve project and program plans submitted by the Supplier.		**x**
6. Authorise the initiation of all projects and Programs.		**x**

READ-ONLY

12. ANNEX A TO SCHEDULE 2.1

12.1. Please see the document 'Annex A to Schedule 2.1 – Circuit Requirements and Locations' attached with the tender documents.

READ-ONLY