The Highland Council

ICT Transition Programme

Data Centre Managed Service

Schedule 2.1a

Part 1 Service Strategy

Data Centre Managed Services

The scope of the Data Centre Managed Service is based on the Supplier adhering to the highlighted Authority ITIL processes, under the relevant sections, these being:

- Part 3 – Service Transition;
- Part 4 – Service Operation;

The scope of the Service defined within the following sections is only applicable for the Data Centre infrastructure components managed by the Supplier.

Section Part 1 – Service Strategy

Service Strategy covers clarification and prioritisation of investment in IT Services to help the organisation to develop and improve over the term of the Agreement.

19 Infrastructure Roadmap

19.1 The Supplier shall, on an annual basis, develop and maintain for the Authority's approval, an infrastructure roadmap that will detail the architecture and upgrade path for the infrastructure components that form the basis of the Services.

19.2 In managing the infrastructure roadmap the Supplier shall consider the need to integrate and apply appropriate future technologies and changes in architectural and security standards.

Section C: Operational Services

Part 2 Service Design
Data Centre Managed Services

Section **Part 2 – Service Design**

Service Design covers the design of IT Services, processes and other aspects of service management. The Supplier's Service Design will address how the planned service solution interacts with the larger business and technical environments, service management systems required to support the service, processes which interact with the service, technology, and architecture required to support the planned service.

20 Availability Management

20.1 The Supplier shall provide Availability Management services to ensure that IT infrastructure, processes, tools and roles are appropriate for the agreed availability targets.

20.2 Availability Management shall include the definition, analysis, planning, measurement and improvement of IT Service availability.

20.3 The Supplier shall ensure the Services are delivered to the agreed availability levels as set out in schedule 2.2a (Performance Levels).

20.4 Following a technical change, the Supplier shall validate that relevant availability, resilience and recovery mechanisms are effective and capable of meeting the agreed Performance Indicators as set out in schedule 2.2a (Performance Levels).

20.5 The Supplier shall provide metrics indicating achieved versus agreed service availability for review by the Authority at the appropriate agreed Board meeting.

20.6 The Supplier shall, on an on-going basis, monitor and track availability performance against targets and Performance Indicators and report to the Authority which areas are performing well and report using the Continual Service Improvement process for those areas in need of improvement.

21 Capacity Management

21.1 The Supplier shall provide a Capacity Management service that considers all resources required to deliver the IT Service, and plans for short, medium and long term business requirements, aiming to ensure that the capacity of IT Services and the IT infrastructure is able to meet the requirements as set out in schedule 2.2a in a cost effective and timely manner.

21.2 The Supplier shall ensure the capacity and performance of IT Services and infrastructure support the agreed Availability Performance Indicators as set out in schedule 2.2a (Performance Levels).

21.3 The Supplier shall use Capacity Management to fulfil future capacity and performance needs.

21.4 The Supplier shall on a monthly basis provide the Authority with a current and future storage capacity and performance position by means of a capacity management report for review by the Authority at appropriate agreed Board meetings.

21.5 The Supplier shall periodically and at a minimum every six calendar months, assess storage capacity and performance of systems and components to identify improvements to ensure optimisation of resources and make available their recommendations using the Continual Service Improvement Process for review by the Authority at appropriate agreed Board meetings.

21.6 The Supplier shall:

21.6.1 proactively provide capacity planning and performance monitoring on all infrastructure components under its control and take action to alleviate any potential capacity or performance pressure points;

21.6.2 size all proposed new systems to determine computing and network resources required;

21.6.3 monitor, and collect capacity statistics and report on a monthly basis including:

21.6.3.1 CPU utilisation;

21.6.3.2 memory utilisation;

21.6.3.3 datacentre network hardware utilisation;

21.6.3.4 datacentre network link utilisation; and

21.6.3.5 storage and back up space;

21.6.4 provide a monthly analysis (as part of the Performance Monitoring Report) to the Authority for all infrastructure components, including performance, capacity, and utilisation;

21.6.5 include forecasts and any recommendations for amendments/upgrades to the infrastructure; and

21.6.6 provide work plans to the Authority (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 Authority with sufficient time to allow the proposed work to be approved, co-

ordinated, resourced and carried out in advance of any impact to the Authority's business operations.

21.7 The Supplier shall ensure that the infrastructure performance monitoring service monitors, captures and analyses real time information from the hardware and software used to deliver the Services to the Authority.

21.8 This monitoring, capturing and analysis shall be based on the Supplier tools, which shall be connected to the Supplier's monitoring and alerting systems. This shall form the basis for both the proactive and reactive capacity and performance reporting leading to any service improvement in highlighted areas.

21.9 Once connected, thresholds shall be provided to the Authority for its approval for each separate element and the proactive monitoring switched on by the Supplier. These dictate the level at which alerts are raised, which shall inform the delivery teams of possible issues via the Supplier's management dashboard and monitoring screens. A 'ticket' (for a Service Incident) shall then be auto raised in the Supplier's service support system. These shall then be reacted to, fixed, and closed down. At all times Service Incident, problem and change processes of the Supplier shall be adhered to and corrective actions stored in the Supplier's support system. This information forms both the core of the monthly reporting pack for Service Incidents, and provides base information for problem management.

21.10 The Supplier Solution shall include a combination of people, processes and tools to provide a comprehensive capacity planning service. The service shall take into account resource, service and business planning (in consultation with the Authority) to provide a comprehensive service that shall provide the following:

21.10.1 Report and plan the need for any increase or reduction in hardware based on Performance Indicators and cost constraints.

21.10.2 Assess new technology and its relevance to the Authority in terms of performance benefits and cost.

21.10.3 Assess new hardware and software products for use by Capacity Management that shall improve the efficiency and effectiveness of the process.

21.10.4 Report to Authority on performance against targets contained in schedule 2.2a.

21.10.5 Recommend resolutions to performance-related Service Incidents and problems.

21.10.6 Carry out ad-hoc performance and capacity studies on request from the Authority.

21.10.7 Carry out or, participate in, risk reviews of potential changes and business plans to minimise the risk of all changes.

21.11 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 Authority's business and service plans. This plan shall be reviewed and revised quarterly by the Supplier and approved by and made available to the Authority and shall be available to authorised End Users.

23 IT Service Continuity Management

23.1 The Supplier shall use IT Service Continuity Management services to reduce and manage the risk from disaster events to an acceptable level and design workable plans for the recovery of IT Services.

23.2 The Supplier shall provide IT Service Continuity Management services as set out in schedule 8.6 (Business Continuity and Disaster Recovery) and this paragraph 23 of this schedule.

24 Information Security Management

24.1 The Supplier shall:

24.1.1 provide Information Security Management services incorporating technical and organisational measures to ensure the confidentiality, integrity and availability of Authority Data and Services as set out in schedule 2.4 (Security Management);

24.1.2 manage all technical security aspects of the systems and infrastructure (and implement appropriate measures to ensure that the infrastructure is protected from deliberate or accidental breach of security) ensuring confidentially of information and data and preventing unauthorised access;

24.1.3 design and ensure the security architecture to protect the Authority from security attacks and threats and notify the Authority immediately of any potential major risk/threat to the Authority's network e.g impending virus attack;

24.1.4 provide a service that embraces the principles and working practices as defined in ISO 27001 and ISO 27002 and any revision or updates to this standard, with the aim

of ensuring the confidentiality, integrity and availability of in-scope Authority Data and in accordance with schedule 2.4 (Security Management);

24.1.5 provide all necessary support and guidance to the Authority on detecting and preventing security Service Incidents and provide such information as is necessary for the Authority to comply with its statutory and business requirements such as PSN and PCI-DSS compliance where such statutory and business requirements fall within the scope of the Services;

24.1.6 provide network security and access controls in accordance with Good Industry Practice and the Authority's specific requirements;

24.1.7 maintain records of all End Users with administration rights or additional access rights authorised by the Authority, and manage and maintain End User access rights in accordance with the Authority instructions and policies and procedures;

24.1.8 technically enforce and manage systems security with immediate notification to the Authority of suspected or identified systems security breaches;

24.1.9 enforce and manage appropriate systems security and protection policies across all Authority systems/assets and infrastructure;

24.1.10 proactively monitor the infrastructure and assets for any internal or external activity which would compromise its security, integrity or availability, including:

24.1.10.1 users gaining or attempting to gain access to the infrastructure which they are not authorised to access; and/or

24.1.10.2 attempts to log onto the infrastructure using invalid passwords, invalid IDs or logical addresses;

24.1.11 notify the Authority within 30 minutes (or such other period as may be agreed in relation to particular types of Service Incidents) of detection of any Service Incidents of suspected, attempted or actual misuse of, or security Service Incidents affecting the infrastructure, including any deliberate attempts of which it is aware to gain unauthorised access to any component of the infrastructure;

24.1.12 where a security Service Incident is detected, either resolve the Service Incident, provide detailed reporting to

the Authority and preventive measures to ensure that there is no re-occurrence within 1 Working Day, or such other period as may be approved by the Authority in relation to particular types of Service Incidents/ applications / infrastructure;

24.1.13 support and configure the Authority's email monitoring, content filtering and website blocking software as directed by the Authority; and

24.1.14 keep a running six month record of all access made via the Internet and email so that the Authority can interrogate the record and identify/attribute inappropriate usage in accordance with schedule 2.4 (Security Management).

24.2 The Supplier's security manager shall be responsible on behalf of the Supplier for all elements of information security within the Authority's infrastructure in addition to:

24.2.1 implementing and managing an information security risk assessment regime to assist PSN compliance;

24.2.2 implementing and managing an information security assurance program;

24.2.3 providing evidence that existing, revised and new procedures, plus work instructions are ISO 27001/2, PSN and DPA compliant;

24.2.4 monitoring security and investigating and reporting security violations and breaches;

24.2.5 ensuring effective Service Incident reporting, management and investigation processes are in place and carried out;

24.2.6 providing specialist advice and guidance to Authority staff on information security, DPA and FOIA Legislation in conjunction with the Authority's information security officer;

24.2.7 delivering protective monitoring and auditing of ICT applications, infrastructure and processes;

24.2.8 promoting and delivering security training and awareness as required and approved by the Authority's information security officer;

24.2.9 delivering the Authority's approved policies, best practice and compliance with appropriate security policies through the development and use of procedures in accordance with Authority instructions; and

24.2.10 compiling and delivering relevant reports, returns and statistics relating to information security and security compliance on behalf of the Authority.

24.3 While undertaking the above duties the Supplier's security manager shall work directly with the Authority's information security officer(s) to ensure a seamless security service is delivered across the whole ICT infrastructure.

24.4 The Supplier's security manager shall provide advice and guidance to the Authority on security related matters including detection and prevention of Service Incidents and keep the Authority abreast of new developments and their relevance to the Authority's infrastructure and systems.

24.5 The Supplier shall undertake and deliver to the Authority relevant Security Tests from time to time (and at least quarterly across the scope of the ISMS) of the security environment to ensure that the security architecture provides an appropriate level of protection from threats and adherence to PSN compliance. One of the quarterly Security Tests per year will be an IT Health Check performed under CESG's CHECK scheme, appropriate for PSN compliance submissions. The process shall include general (physical) security controls, staff and learner awareness, secure area access, back-up processes, network and server vulnerability scans and firewall and router/switch configurations. The Supplier shall use a mix of inhouse audit and technical skills, along with industry standard tools to both conduct the investigation and produce the final report. The Supplier shall develop an overall plan for PSN compliance assessments setting out any requirements on other parties as reasonably believed to be necessary. The Authority shall approve and disseminate that plan to those parties and shall require and manage their compliance with the stated requirements and timescales.

24.6 The Supplier shall manage and administer various components securing the Authority's applications and infrastructure including:

24.6.1 firewalls;

24.6.2 anti-virus controls;

24.6.3 authentication, authorization and accounting systems;

24.6.4 intrusion detection and prevention systems;

24.6.5 network access ;

24.6.6 management of user access rights; and

24.6.7 security logging.

24.7 The Supplier shall implement and use effective e-mail and internet content filtering and blocking systems (where appropriate) and remove illegally downloaded software where detected and as agreed with the Authority residing on Authority assets across the Authority's infrastructure and systems.

24.8 The Authority will authorize and approve logon/security level access for Authority and Supplier employees, agents, and subSuppliers.

24.9 The Supplier shall maintain physical and logical security of facilities, networks, systems, data and assets.

27 Service Level Management

27.1 The Supplier shall provide Service Level Management services to ensure performance against Performance Indicators as defined in schedule 2.2a (Performance Levels) are monitored, measured and reported on.

27.2 The Supplier shall ensure Operational Level Agreements ("OLAs") and Underpinning Contracts ("UCs") whether subcontracted by Supplier, COTS contracts with third parties for which the Supplier is the named party on behalf of the Authority for use of the COTS by the Authority and/or End Users, or contracts with HC Notified Suppliers managed by Supplier for or on behalf of the Authority within the scope of the Services, are appropriate, documented and maintained and reviewed with the Authority on an annual basis. The Supplier will also in conjunction with the Authority review OLAs and UCs put in place by the Authority covering HC Managed Suppliers. Where OLAs and/or UCs do not support the agreed Service Level requirements, the Authority and the Supplier shall agree on the course of action.

27.3 The Supplier shall provide the Authority with Performance Monitoring Reports in accordance with schedule 2.2a (Performance Levels).

27.4 The Supplier shall where requested and required by the Authority produce regular reports to assist in the measurement of performance and/or availability of specific systems integral to the delivery of customer facing services.

27.5 The Supplier shall on an on-going basis monitor and track performance against Performance Indicators to both demonstrate to the Authority which areas are performing well and report using the Continual Service Improvement Process (see Part E of this schedule 2.1a) those areas which may be threatened and need improvement.

27.6 The Supplier shall provide performance and customer satisfaction information for the Services to the Authority to

enable the Authority to complete benchmarking surveys as required.

27.7 The Supplier shall provide assurance and evidence to the Authority that sub-contracts are approved by the Authority and service acceptance criteria are fulfilled at Implementation Services Commencement Date.

Part 3 Service Transition
Data Centre Managed Services

Section Part 3 – Service Transition

Service transition covers the processes to deliver IT Services into live/operational use both for Implementation Services and on-going Service transition throughout the duration of the Agreement.

The scope of the Data Centre Managed Service is based on the Supplier adhering to the highlighted Authority ITIL processes, these being:

- **Change Management;**
- **Knowledge Management;**
- **Release and Deployment Management;**
- **Service Asset and Configuration Management;**

Part 4 Service Operation

Data Centre Managed Services

Section Part 4 – Service Operation

Service Operation provides for the delivery of IT Services to agreed levels of service to Authority and End Users.

The scope of the Data Centre Managed Service is based on the Supplier adhering to the highlighted Authority ITIL processes, these being:

- **Incident Management;**
- **Problem Management;**

36 Access Management

36.1 The Supplier shall provide an Access Management service which applies and enforces the Authority's IT Security / Information Security Management policies with the aim of granting authorised users the right to use a service, while preventing access to non-authorised users.

37 Event Management

37.1 The Supplier shall provide an Event Management process to constantly monitor services and filters and categorises Events in order to decide on appropriate actions.

37.2 Event Management shall include:

37.2.1 a mechanism for generating, filtering, correlating and responding to Events;

37.2.2 communication of warning and exception Events;

37.2.3 consolidated logging of warning and exception Events;

37.2.4 validation that Events have been handled appropriately and may be closed; and

37.2.5 Identification and implementation of corrective action based on trend and pattern analysis; and

37.2.6 The correlation of Events that indicates infrastructure unavailability will trigger an appropriate incident and classification in relation to any of the infrastructure defined in Schedule 2.2a, part 7 Infrastructure Availability.

37.3 The Supplier shall investigate security breaches, providing information as required from the consolidated logs and report the outcomes of investigations to the Authority.

39. IT Operations Management

39.1 The Supplier shall provide IT Operations Management services and deliver the day-to-day technical supervision of the IT infrastructure and applications and work from documented processes and procedures.

39.2 The Supplier's IT Operations Management service will deliver the following:

39.2.1 a stable and secure IT infrastructure;

39.2.2 a log of all operational events;

39.2.3 maintenance of operational monitoring and management tools; and

39.2.4 provision of operational scripts and procedures.

39.3 The Supplier will:

39.3.1 use appropriate tools to proactively monitor, optimise and support the infrastructure and applications on a continuous basis to prevent or minimise any failures and to support service provision to Performance Indicators;

39.3.2 control and load media onto the infrastructure including storing and moving backup media to and from storage;

39.3.3 take all reasonable actions to optimise the performance of the infrastructure;

39.3.4 change configuration of infrastructure elements as authorised by the Change Management process carry out and document all housekeeping jobs (e.g. user administration, back-ups, message clearing, re-booting and performance monitoring) for the infrastructure; and

39.3.5 pro-actively provide advice and guidance to the Authority

with regard to any improvements that can be made in the light of changes in technology to the Authority's configurations for the infrastructure.

39.4 The Supplier shall proactively manage the availability of the Authority's infrastructure under its direct control.

39.5 All infrastructure for the Authority shall be maintained in a secure and controlled environment suitable to sustain the infrastructure and to comply with the Performance Indicators. The infrastructure shall be maintained in line with manufacturer recommendations.

39.6 The Supplier shall utilise system management tools to provide proactive monitoring of the infrastructure. This monitoring shall be configured to proactively monitor the infrastructure and alert the Supplier automatically of any Service Incidents.

39.7 The Supplier shall perform regular maintenance tasks on all infrastructure components which shall be undertaken in line with the Supplier's best practice and Good Industry Practice.

39.8 Additional infrastructure services which the Supplier shall provide include:

39.8.1 maintenance of supported versions of infrastructure component software. This involves the application of operating system patches and firmware upgrades as recommended by the vendor;

39.8.2 monitoring infrastructure components resource trends to proactively avoid affecting services;

39.8.3 responding to operating system related problems and taking corrective action in a controlled manner;

39.8.4 on-going performance tuning of the infrastructure components operating systems; and

39.8.5 monitoring of infrastructure components system log files to detect system problems.

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

39.10 The Supplier shall:

39.10.1 provide monthly availability and capacity reports as part of the Performance Monitoring Report;

39.10.2 attend strategy and operational meetings as defined in the schedule 8.1 or otherwise agreed with the Authority;

39.10.3 provide on-going advice if requested by the Authority;

39.10.4 facilitate briefing sessions, to the Boards specified in schedule 8.2 providing a summary of technology and service advances that may benefit the Authority in respect to improving the services that are delivered or reducing the costs of delivering services, and provide a Service Improvement Plan on an annual basis, within 20 Working Days of the end of each Contract Year. This plan will be monitored and adjusted on a monthly basis if required;

39.10.5 review and align media operations, control, loading and storage to a best practice model that fulfils the Authority's requirements set out in this Agreement; and

39.10.6 investigate, and make recommendations for an ongoing programme of infrastructure optimisation targeted at delivering the optimum performance from each of the service component elements.

40 Operational Hours

40.1 The Supplier shall ensure operational support for the Services is provided during the following Operational Hours:

40.1.1 Service Request support availability 0800 – 1800 on Working Days;

40.1.2 Service Request and Incident logging 0000 – 2359; (24x7 x 365);

40.1.3 Severity 2 Incidents, Severity 3 Incidents, and Severity 4 Incidents support availability 0800 – 1800 on Working Days;

40.1.4 Severity 1 Incidents (24x7 x 365); and

(All of the above being "**Operational Hours**").

40.2 The Authority can request operational support for the Services outside of Operational Hours and/or on non-Working Days through the Service Request process.

42 Request Fulfilment

42.1 The Supplier shall provide a Service Request process to fulfil Service Requests these will be defined as:

a. Catalogue – costs for implementation are included in the standard service offering as defined in Schedule 2.2a;

b. Non-Catalogue – costs for implementation are provided via quote;

c. Contract Changes - in accordance with the Change Control Procedure as set out schedule 8.2 (Change Control Procedure).

42.2 The Supplier's delivery of the Service Request fulfilment shall include:

42.2.1 effective and efficient handling of Service Requests;

42.2.2 recording and categorisation of Service Requests with appropriate diligence and processing within the agreed time schedule in accordance with schedule 2.2a (Performance Levels) and schedule 8.2 (Change Control Procedure), where applicable;

42.2.4 continuous monitoring of Service Request status to prevent breach of Performance Indicators; and

42.2.5 quality assurance of a Service Request as it is managed throughout its lifecycle.

42.3 The Supplier will pass onto the Authority, on an open book, auditable and justifiable basis, any volume discount obtained by the Supplier for fulfilment of a Service Request, subject to the terms of such volume discount agreement.

42.4 The Supplier will run vendor and cost/price comparison benchmarking reviews for all Service Requests and

ensure the Authority obtains competitive pricing for the purchase of services pursuant to such Service Requests.

43 Service Reporting and Service Review Services

43.1 The Supplier shall:

43.1.1 collate and format service performance statistics and supporting information in a format agreed with the Authority;

43.1.2 prepare and publish adequate and accurate service Performance Monitoring Reports (in accordance with this schedule 2.1a and schedule 2.2a (Performance Levels)) to demonstrate delivery against the Performance Indicators for each of the Services;

43.1.3 provide monthly Performance Monitoring Reports to the Authority by the end of the 5th Working Day of the new calendar month unless agreed otherwise;

43.1.9 provide monthly Performance Monitoring Reports to the Authority by the end of the 5th Working Day of the new calendar month unless agreed otherwise;

43.1.10 conform to the Authority's report review requirements which may result in changes to the content, format and timing of such reports; and

43.1.11 Measure and analyse performance relative to requirements.

43.6 The Performance Monitoring Report shall contain, as a minimum, all of the information as set out in schedule 2.2a (Performance Levels).

43.7 The Supplier's service review shall include the following:

43.7.4 **Monthly and Quarterly Service Reviews**

The Supplier shall provide the monthly Performance Monitoring Reports and quarterly summaries and participate in monthly Performance Review Meetings in accordance with schedule 2.2a (Performance Levels).

43.7.6 If the Authority is satisfied with the Performance Monitoring Report, quarterly summary and/or Annual

Review Report issued by the Supplier, the Supplier shall forthwith implement the proposals set out in the relevant Service Report (including any actions which have been identified) in accordance with the timescales set out in the Service Report. If the Authority is not satisfied with the Service Report, the Authority shall request amendments or clarifications and the Supplier shall make such amendment or provide such clarification of the relevant Service Report as requested by the Authority within ten (10) Working Days of the request by the Authority.

Where a Service Report contains a recommendation or proposal for variation of Performance Indicator(s), then if the Authority (at its sole option) accepts such recommendation or proposal, the Parties shall vary the relevant Peformance Indicator(s) in accordance with the Change Control Procedure.

44 Service Management

44.1 The Supplier shall provide an ISO/IEC 20000-aligned Service to support Incident, Problem management and Service Requests in relation to Data Centre Managed Service.

44.3 The Supplier will:

44.3.1 provide the ability the Authority's Service Desk to log contacts;

44.3.3 co-ordinate fault resolution and Service Incident management for all Service Incidents and enquiries relating to the agreed Services;

44.3.4 adhere to the Service Asset and Configuration Management process as defined in Part 3 Service Transition for for all Authority Assets relating to the agreed Services

44.3.6 use appropriate management systems and tools to enable the Authority's Service Desk contacts to be logged, tracked, analysed and escalated;

44.3.8 provide a web based system which shall allow the Authority's Service Desk to log and track all support Incidents and Requests;

44.3.9 notify the Authority of contact resolutions and closure for all Severity 1 Service Incidents and via email;

44.3.10 notify the Authority via SMS text of open and closed Severity 1 Service Incidents and to a designated list of Authority staff;

44.3.11 identify and highlight root cause of Severity 1 Incident and Severity 2 Incident level problems or failures and recommend appropriate resolution action, where/whenever possible;

44.3.12 substantiate to the Authority that all reasonable actions have been taken to prevent recurrence of such failures;

44.3.13 track and report on progress of all Severity 1 Incidents and Severity 2 Incidents that are escalated to Level 2 support to ensure that Root Cause analysis is performed and reported on;

44.3.14 provide the Authority with a written report detailing outstanding problem tickets; provide updates on a monthly basis until closure;

44.4 The Supplier shall:

44.4.1 perform capacity monitoring and planning to ensure appropriate levels of staff to deliver the Service in accordance with Targets defined in Schedule 2.2a;

44.4.2 perform staffing analysis to ensure personnel have the appropriate sets of skills, training, and experience in line with Authority capacity and technology; and

44.4.3 install/test/maintain the Supplier's Service Desk systems and portals.

45. Technical Management

45.1 The Supplier shall provide Technical Management services that deliver technical expertise and support for the management of the infrastructure.

45.2 Technical Management shall include:

45.2.1 designing, testing, operating and improving Services;

45.2.2 maintaining skills required to operate the infrastructure required;

45.2.3 technical management of every key technology area of the infrastructure; and

45.2.4 responsibility for the technical aspects of designing, testing, operating and improving IT Services.

45.3 The Supplier shall document all hardware and software configurations including HLD's/LLD's on the Authority's management systems

45.4 The Supplier shall provide on-going advice, at the Authority's request in respect of the infrastructure availability, performance, utilisation and capability to support new applications and business initiatives.

45.5 On a six monthly basis the Supplier shall review the levels of software and firmware running on the infrastructure and produce a report as part of the relevant month's Performance Monitoring Report. The report shall:

45.5.1 provide a high level summary of the current infrastructure software and firmware levels; and

45.5.2 identify components where there is a potential issue with respect to the current level of software and firmware and its potential ability to negatively impact the performance of the infrastructure along with recommendations to address those weaknesses.

45.6 The Supplier shall undertake physical audits of the infrastructure as required by the Authority from time to time and produce audit reports in the format as specified by the Authority.

45.7 The Supplier shall assign a Lead Architect to oversee technical implementation and change.

Part 5
Continual Service Improvement
Data Centre Managed Services

Section Part 5 – Continual Service Improvement

Continual Service Improvement uses methods from quality management in order to learn from past successes and failures with the aim of continually improving the effectiveness and efficiency of IT processes and services.

The Supplier will carry out Service Improvement as set out in Clause 8 of this Agreement.

Part 6 Service Components

Data Centre Managed Services

Section Part – 6 Service Components

This part sets out the individual components of service and the requirements which the supplier must deliver.

49 Application Support

49.13 The Supplier shall provide operating platform, technical and operating system support and maintenance for the infrastructure that underpins the supported applications.

53 Authority Data – Format

53.1 The Supplier shall ensure Authority Data is returned either on expiry or earlier termination in a format that is non-proprietary and uses methods that conform to industry standards.

54 Backup and Recovery Services

54.1 The Supplier shall provide backup and file restore services to support all services to the agreed performance levels set out in Schedule 2.2a.

54.2 The Supplier shall ensure backup data availability and related restore capability are maintained in accordance with the Authority's "Corporate Records Retention and Destruction Policy" as notified by the Authority.

54.3 The Supplier shall ensure there is no impact on network performance or availability of Authority services and End User services during normal business hours as a result of running or over-running system backups.

54.4 The Supplier will:

54.4.1 agree backup schedules, retention arrangements and working practices with the Authority to meet the Authority's business and statutory requirements and implement as necessary;

54.4.2 provide appropriate on and off-site back-up of all appropriate applications so that all data on these applications can be reconstituted. Back up procedures shall be based on good industry standards, including standards regarding integrity and frequency and physical location, as well as the Authority's reasonable, specific requirements;

54.4.3 ensure appropriate daily and weekly and other required frequency back-ups are taken of all applications. The backup media used may form a part of any disaster recovery strategy drawn up by the Authority. All backups to be moved and stored in an appropriate, secure offsite

facility before start of business hours the following working day;

54.4.4 provide, manage and support appropriate corporate backup and restore tools;

54.4.5 backup all software (including configuration data) and data before and after any change or maintenance is carried out;

54.4.6 provide a data restoration service, as approved by the Authority;

54.4.7 provide all consumables necessary for the provision of the backup service;

54.4.8 carry out regular test restores on a monthly basis for a variety of applications and databases; and

54.4.9 at any time with reasonable notice, demonstrate to the Authority as part of the regular monthly test restore cycle that effective restore from the backups can be done which may include a random selection of files.

54.5 The Supplier shall review all the current processes, scripts, mechanisms, software and hardware against current best practice, Good Industry Practice, the business requirements of the Authority and the Supplier will create a list of short, medium and long term actions required to deliver a comprehensive backup service. The recommendations from this exercise shall feed into the Service Improvement Plan and be discussed with and approved by the Authority and the relevant actions instigated.

54.6 The Supplier will notify the Authority during the Implementation Services of anything that requires immediate action and remedied before the service commencement date as approved by the Authority.

54.7 The system management toolsets the Supplier shall employ on the Authority infrastructure estate shall provide backups of the infrastructure configurations to ensure these are both restorable and remotely deployable in the event of an issue arising from either hardware failure or as result of a change

54.8 The Supplier shall facilitate and manage the off-site, secure storage of backup media.

54.9 Fulfilment of data backup or restoration requests

70 **Gateway Services**

70.1 The Supplier shall provide reliable and consistent connectivity to corporate systems using approved devices from any location to the extent the connectivity is within the control of the Supplier in accordance with schedule 2.2a (Performance Levels).

70.2 The Supplier shall ensure security is maintained to local and central government standards ensuring compliance is assured at all times.

70.3 The Supplier shall ensure services achieve or exceed agreed Performance Indicators.

70.4 The Supplier shall design and maintain Gateway Services to avoid lengthy authentication processes, provide session persistence and support alternative methods of device connectivity.

70.5 The Supplier shall operate network access controls which control the access of users to Authority systems. Where applications support it, this information should be passed by Gateway Services to those applications.

70.6 The Supplier shall operate a secure certification key system that enables Endpoint Devices to be distinguished by the network access controls.

70.7 The Supplier shall operate network access controls for approved third parties using their own devices.

71 **Hosting Services**

71.1 The Supplier shall provide system and solution Hosting Services including servers and storage to support the Performance Indicators set out in schedule 2.2a (Performance Levels) for the applications as notified by the Authority.

71.2 The Supplier shall provide and support production, test and patch development and any other environments as requested by the Authority.

71.3 The Supplier shall:

71.3.1 ensure all infrastructure level components are designed and configured to achieve or exceed the agreed Availability Performance Indicators set out in schedule 2.2a (Performance Levels);

71.3.2 ensure compliance with the Authority's information security requirements;

71.3.3 provide operations management including the liaison with third-parties in the resolution of Service Incidents; and

71.3.4 ensure there is no corruption or loss of any Authority Data hosted on the Hosting Services.

71.4 Where hosting is provided outside of the Authority Premises the Supplier will ensure that such externally hosted systems and solutions must be:

71.4.1 capable of integrating with the Supplier's Service Management processes;

71.4.2 aligned to the Authority Requirements stated in this schedule; and

71.4.3 capable of maintaining existing data interchange between systems.

71.5 The Supplier will:

71.5.1 ensure the site or sites utilised by the Supplier have sufficient scalability and capacity to allow for the implementation and installation of new systems (and upgrades or new versions of existing systems) to accommodate the reasonably likely future requirements of the Authority (such requirements to be the basis of typical local authority of its size and functions) without the Authority being liable for any additional site costs;

71.5.2 ensure that the ICT hosting infrastructure is resilient, at least in accordance with current Good Industry Practice;

71.5.3 ensure that the ICT hosting infrastructure shall perform to meet agreed user response requirements.

71.5.4 Utilise resilient WAN datacentre links and support arrangements from Authority;

71.5.5 suggest the most appropriate Infrastructure platform or service; and

71.5.6 work with the Authority within PSN/CESG approved management policies.

74 Perimeter and Network Security and Support Services

74.1 The Supplier shall support all network services under its control required to achieve or exceed Performance Indicators set out in schedule 2.2a (Performance Levels), to include:

74.1.1 Firewalls, VPN, routing, switching and load balancing infrastructure, DMZs and other network zones, web and e-mail content filtering and management systems,

proxies, intrusion detection/prevention and other controls to support agreed security levels;

74.1.2 The Supplier shall configure and manage all firewalls, maintain firewall rule base and apply security upgrades and patches as required in a timely manner to maintain the security architecture. The Supplier shall maintain, and update changes approved by the Authority including domain names, address ranges, URLs, network, End Users and End User groups; and

74.1.3 ensure all firewall rules are documented and have a full explanation for their existence and undertake firewall changes as directed and agreed by the Authority.

74.2 The Supplier's roles and responsibilities shall include but not be limited to:

74.2.1 ensuring the Authority's security architecture is patched up-to-date against latest security attacks and threats by deploying necessary security patches, fixes and configuration changes;

74.2.2 tracking the managed estate for any known vulnerabilities by monitoring various information security advisory and product vendor's web sites and by other means;

74.2.3 identifying vulnerabilities and their risks and mitigating the risk by identifying the solutions / workaround;

74.2.4 coordinating with the respective asset owner / custodian the implementation of the solution;

74.2.5 ensuring security policies practised are in line with the Authority's corporate security policies;

74.2.6 define services and adhere to standards for Data environment for approval by the Authority; and

74.2.7 providing recommendations to improve upon security management and administration in-line with PSN compliance.

74.2.8 The Supplier will be responsible for managing and maintaining:

74.2.8.1 perimeter defences and services, including firewalls and intrusion detection/prevention services; and

74.2.8.2 perimeter access services, including AAA services, VPN access servers and remediation servers;

74.2.8.3 perimeter content delivery services including reverse proxy and publishing services utilising Supplier provided toolsets; and

74.2.8.4 secure domain and server isolation domains (using NAP and certificate services) within the network for secure services such as Government Connect Mail.

74.3 The Supplier will review the existing controls over external/third party access and identify any weaknesses or opportunities for improvement on an on going basis.

74.4 The Supplier will continue to develop and provide the remote access capability while maintaining a secure environment.

74.5 The Supplier shall be responsible on behalf of the Authority for all elements of information security within the Authority's infrastructure and applications that are under the Supplier's direct control.

74.6 The Supplier shall manage, maintain and support as a minimum the following:

74.6.1 firewalls and intrusion detection and prevention devices;

74.6.2 authentication, authorisation and accounting systems;

74.6.3 access services such as VPN and Citrix gateways;

74.6.4 proxy services;

74.6.5 content delivery services;

74.6.6 network access and isolation; and

74.6.7 Government Connect mail.

74.7 The Supplier will participate in defining services and standards for planning and analysis activities in respect of perimeter security, which will be delivered to the Authority for its approval.

74.8 The Supplier will define services and adhere to standards for Data environment as approved by the Authority.

74.9 The Supplier will perform business liaison function to network carrier for capacity planning and analysis.

74.10 The Supplier will perform technical planning with Authority staff for capacity that impacts performance for LAN/WAN services.

74.11 Set up remote access

78 Public Services Network (PSN)

78.1 The Supplier shall maintain connectivity to the PSN and Government Gateway service that satisfies the PSN requirements, as notified by the Authority and any other technical requirements necessary for these services, through a regime of appropriate annual health checks and assessments that may be required by the PSN and carry out any remedial action required to achieve the PSN standard.

78.2 The Supplier shall maintain compliance of the Services with the PSN standards for data security and ensure the terms of the PSN Code of Connection, as notified by the Authority, are not breached. This will include, and not be limited to, ensuring compliance with protective monitoring, security Service Incident and Event Management, situational awareness, risk management, Change Management and Release Management and service management relating to the Data Centre scope.

78.3 PSN Services will be delivered in accordance to the PSN standards, accredited to the appropriate level by CESG and comply as a minimum to Business Impact Level of IL2 for Confidentiality and Integrity.

78.4 The Authority will be responsible for the PSN submission and accreditation. The Supplier shall provide a plan covering the Data Centre and their responsibilities in gathering data and undertaking testing to provide their relevant areas of the submission. The Authority shall manage the provision of such data by other service providers, and the Supplier shall discharge its own responsibilities in this respect all required information to the Authority for the Authority to make its submission. This will include, and is not limited to, outputs from network and system audit information, security and vulnerability assessments, and change and remediation logs.

For the avoidance of doubt, the Authority will be responsible for the third-party costs associated to the completion of the IT Healthcheck. In accordance with the output from the IT Healthcheck from 24.5, the Supplier will remediate all relevant actions associated to the scope of the service, excluding hardware, at the Suppliers cost.

80 Software License and Certificate Management

80.1 The Supplier shall be responsible for the management of licenses and certificates for applications provided by the Supplier or deployed by the Supplier to Authority approved devices, including:

80.1.1 maintaining records of licenses and certificates held and deployed and provide a monthly statement to the Authority;

80.1.4 providing information needed by software vendors to undertake software audits under the terms of the license agreements.

80.3 The Supplier will:

80.3.2 procure software licences required in order for the Authority to receive the Services in accordance with this Agreement. This shall be subject to the Supplier utilising any volume discount agreement which the Supplier may benefit from, which shall be demonstrated to the Authority on an open book, auditable and justifiable basis. The Authority may elect to procure a direct licence of any software in the event that the Authority is able to obtain a more favourable rate, however the Supplier shall (unless agreed otherwise) remain responsible for integrating, implementing, maintaining and/or supporting such software; and

80.3.3 inform the Authority of any known unlicensed software being used and details of any unused software licences;

80.4 where the Supplier is unaware whether a software instance is licensed, to make all reasonable endeavours to determine the software licence status. This includes but is not limited to checking with the person responsible for the purchase of the hardware or software and where appropriate record the software on the asset management system and Authority license software tool;

80.5 make sure that software licence details procured either by the Supplier or the Authority are recorded for all relevant components in the CMDB and make sure evidence of ownership and/or proof of ownership is provided by the software owner;

80.6 liaise with the software suppliers to take out or renew software licences as required to meet the Authority's requirements;

80.8 maintain an organised library of software licences, manuals, documentation, software installation CDs and discs for current and (at the Authority's request) previous versions of the software. This to be made available to the Authority upon request;

80.9 ensure that all licences required for the Authority are managed properly in accordance the licensors' requirements and obtained lawfully in line with the software licensor's policy;

80.10 make sure that all new or replacement software is made available at the point of use;

80.14 The Supplier shall provide the following services:

80.14.2 The Supplier shall create an effective licence position report detailing the Authority software entitlement position by vendor, product, version and licence on an annual basis, delivered within 20 Working Days of the end of each Contract Year.

80.15 The Supplier shall provide on a monthly basis and as part of the Performance Monitoring Report, an 'Entitlements Report' detailing all of the Authority's entitlements at that point in time. The Supplier shall track the Authority's entitlements, giving opportunities to:

80.15.1 exploit the latest vendor licensing schemes, roadmaps of planned changes and product releases;

80.15.2 align entitlements to the Authority's actual requirements;

80.15.3 identify under-used agreement options and benefits entitlements;

80.15.4 recommend renewals and consolidation opportunities; and

80.15.5 identification of potential renegotiation levers.

80.16 The supplier shall be responsible for holding the DSL where all issue media shall be stored in regards to DC services.

80.17 Microsoft Licensing Assistance - The Supplier shall on behalf of the Authority, compute the best fit licensing model for Microsoft products. This can be a combination of different agreements covering both the Authority's Corporate and Curriculum environments.

CR125 The scope of activities for THC PKI infrastructure include:

- Maintain Microsoft Servers;
- Maintain signing algorithm to latest standards;
- Maintain Microsoft Root CA, Issuing CA and Certificate Revocation List Server;
- Maintain the integration Issuing CA with Active Directory
- Maintain the respective certificate templates for the Suppliers infrastructure;

81 Software Patch Management

81.1 The Supplier shall be responsible for patching of firmware, operating systems, database platforms, and supplier managed applications.

81.3 As a minimum the Supplier shall deploy critical and security patches (or equivalent classification dependent on vendor) and in accordance with the Change Management process.

81.4 The Supplier shall ensure that the requirements of PSN and PCI compliance are maintained through an effective patching regime where systems fall within the Supplier's scope of service.

82 Storage Management

82.1 The Supplier shall provide Storage Management services that ensure storage achieves or exceeds the agreed individual or aggregated system Performance Indicators as set out in schedule 2.2a.

82.2 The Supplier's Storage Management services will ensure demand and capacity are effectively managed to maintain service availability and optimum utilisation of storage assets.

82.3 The Supplier shall ensure storage Problems and Service Incidents are managed to minimise service unavailability and ensure performance against Performance Indicators as set out in schedule 2.2a (Performance Levels).

83 Threat Management

83.1 The Supplier shall provide and support internet security gateway infrastructure and related services providing real-time, online threat analysis to defend against advanced malware and blended threats.

83.2 The Supplier shall ensure appropriate controls are in place to administer group and End User based internet restrictions. The Authority will use the Service Requests process to request changes to these access restrictions which will be included in the scope of this Service.

83.3 The Supplier shall immediately escalate to the Authority notified threats involving risk to reputation, compromised security; financial risk; or injury to be treated as Severity 1 Incidents.

Section D Optional Services

Data Centre Managed Services

Section D – Optional Services

This section sets out the Optional Services which the Authority may request the Supplier to provide.

The following optional services will be in scope:

- Project Management;
- Procurement;
- Consultancy;

Costs would be based on the agreed rate card

Section E Glossary

Data Centre Managed Services

Section E – Glossary

Access Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Active Directory means the Microsoft Active Directory;

Application Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Application Portfolio has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011 ;

Availability Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Business Relationship Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Capacity Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Catalogue Service means a defined and costed entry in the Supplier's Service Catalogue;

CESG means the Communications-Electronics Security Group within GCHQ;

Change Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Configuration Items or **CIs** has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Configuration Management Database or **CMDB** has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Configuration Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Continual Service Improvement has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Corporate means the Authority's head office, office users and External Customers of the services;

Curriculum means the Authority's school, learning, teaching and education users of the services;

Demand Management has the meaning given in ITIL Glossary

of Terms, Definitions and Acronyms 2011;

Design has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

DHS means the definitive hardware store;

DSL means the definitive software library;

Endpoint Devices means the devices supplied for End Users to access the services. These include: desktop computers, laptop computers, tablets/cloud optimised devices, and associated IT Peripherals supplied with the hardware (for example mice, docking stations, monitor cables);

Endpoint Device Break-Fix means the service provided by the Supplier to resolve Service Incidents with Endpoint Devices;

Endpoint Device Recovery & Disposal means the services set out in paragraph 65 of schedule 2.1;

Endpoint Device Pool means the services set out in paragraph 64 of schedule 2.1;

Endpoint Device Security means the security services and protections provided by the Supplier to ensure Endpoint Devices are secure;

Endpoint Device Supply means the supply of Endpoint Devices pursuant to paragraph 61 of schedule 2.1;

Event has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Framework Services means the services in respect of End User Devices, IT Peripherals and IT Consumables which will be procured by the Authority using third party suppliers as set out in paragraph 60.1 of schedule 2.1;

Framework Suppliers has the meaning set out in paragraph 60.1 of schedule 2.1;

Event Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011);

Gateway Services means the services set-out in Part 6 of this schedule 2.1a;

Government Gateway means the points of entry and return to secure UK government IT infrastructure as referenced at paragraphs 68, 70 and 78 of schedule 2.1;

Highland Council Services means services provided by the

Authority, including Care and Learning, Education and Finance;

Hosting Services means the services required under Part 6 of this schedule 2.1a;

IMAC means the Implementations, Moves and Changes Services;

Incident(s) has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011 ;

Incident Closure Procedure means the procedure adopted by the Supplier to formally close a Service Incident;

Incident Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Information Security Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011 ;

ISO 27001 means the international Standard that describes best practice for an information security management system;

ISO 27002 means the international standard that describes best practice for information security management;

IT Operations Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

IT Consumable means an which is supplied to End Users on an ad-hoc basis, including recordable CDs, DVDs and memory sticks.

IT Peripherals means the items supplied to End Users on an ad-hoc basis, and not part of a bundle with Endpoint Devices, this includes mice, docking stations, monitor cables, audiovisual equipment.

IT Service Continuity Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Knowledge Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Known Error has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011 (or equivalent);

Known Error Database has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Lead Architect means the designer of the Supplier's technical solution;

MPS Provider" means Xeretec Limited, a party with which the Authority has entered into an agreement for the provision of MPS, or such other party as the Authority may appoint for the provision of MPS from time to time;

Office Service means the services used by Corporate service users;

Operational Level Agreements or **OLA** has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Optional Services means the services set out in section D of this schedule 2.1a;

PCI -DSS means the Payment Card Industry Data Security Standard;

Performance Monitoring Report means the reporting arrangements provided by the Supplier (in accordance with this schedule 2.1a and schedule 2.2a (Performance Levels);

Personalised Mail Supplier means the Authority's personalised mail service supplier and the Authority's personalised mail supplier's print partner;

Personalised Print means print services procured by the Authority in relation to printing services;

PID means the project initiation document;

PRINCE2 is the standard UK government methodology for Project management;

Problem has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Problem Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

PSN means the Public Service Network;

Public Sector Programme Management Approach means the published programme management approach developed for regional and central government

Release has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Release & Deployment Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Release Management has the meaning given in ITIL Glossary

of Terms, Definitions and Acronyms 2011;

Request Fulfilment has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Root Cause has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

School Services means the services used by the Curriculum service users;

Service Asset and Configuration Management ("**SACM**") has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Catalogue has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Design has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Desk has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Improvement Plan means a plan setting out the details of the action which the Supplier proposes to take to improve its performance including in the areas for improvement identified by the service review meeting and shall set out the timescales for taking that action. This is to be included in the Annual Review Report;

Service Portfolio has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Level Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Report means a report of the achievement and trends against the Performance Indicators;

Service Request has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Service Validation & Testing has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Severity 1 Service Incidents has the meaning defined in paragraph 4.5 of Part 2 of schedule 2.2a (Performance Levels);

Severity 2 Service Incidents has the meaning defined in paragraph 4.5 of Part 2 of schedule 2.2a (Performance Levels);

SWAN means the Scottish Wide Area Network (SWAN)

Framework Contract awarded to Capita plc in February 2014;

Technical Management has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Transformation Programme means the six Transformation Projects sets out in Section B of this schedule 2.1a;

Transition Plan has the meaning set out in schedule 6.1;

Transition Planning and Support has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011;

Underpinning Contracts or **UC** has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011; and

Upgrade Assessment Procedure has the meaning given in ITIL Glossary of Terms, Definitions and Acronyms 2011.