Ministry of JUSTICE

Hosting Services

Schedule 2.1: Service Requirements

TABLE OF CONTENTS

Requirement No.	Level	Requirement
		1. GLOSSARY OF TERMS
		PLEASE REFER TO SCHEDULE 1 AND THE TOWER SERVICE AGREEMENT FOR DEFINITIONS
		2. INTRODUCTION
		2.1 This schedule details the Hosting Services that shall be provided by the Hosting Supplier to the Authority.
		2.2 The structure of this schedule is as follows:
		2.2.1 Section 3 describes the objectives for the Hosting Supplier requirements within the FITS procurement;
		2.2.2 Section 4 describes, at a summary level, the scope of Hosting Services;
		2.2.3 Section 5 describes the structure, function and purpose of the requirements, the significance of each of the levels in the requirements and the purpose of the columns in the requirements tables;
		2.2.4 Section 6 sets out the general principles that need to underpin the Hosting Supplier proposed solution to deliver the obligations set out in the requirements section;
		2.2.5 Section 7 provides details of the FITS strategic themes;
		2.2.6 Section 8 provides details of the FITS TOM design principles for Hosting Services;

Requirement No.	Level	Requirement
		2.2.7 Sections 9 through 22 set out the requirements for the Hosting Supplier; and
		2.2.8 Annex 1 sets out the social value requirements.
		3. OBJECTIVES
		3.1 To define the scope of the Hosting Supplier function in relation to the Other FITS Suppliers and the Authority that make up the FITS TOM.
		3.2 To provide a comprehensive list of requirements for the Hosting Supplier within the FITS Programme TOM construct.
		3.3 To provide key information about the Authority's desired capabilities of a Hosting Supplier.
		3.4 To establish responsibilities for the ongoing management and support of ICT Environments, systems and FITS Services, as defined in the FITS TOM.
		3.5 To support the establishment of the Hosting Supplier proposed approach and formation of its strategy in managing the delivery of Hosting Services under the Hosting Supplier contract.
		3.6 Define the scope of Hosting services within this schedule and directly referenced which describes a principle of on-going service as originally defined originally in the DISC service model.
		4. SCOPE OF HOSTING SERVICES
		4.1 The Hosting Supplier shall be responsible for the supply of FITS Services provided from centralised data-centre facilities; these responsibilities include, but are not limited to:

Requirement No.	Level	Requirement
		4.1.1 The provision, management, maintenance, support and Documentation of Hosting Services;
		4.1.2 ICT Environment hosting within centralised data-centres;
		4.1.3 Provision, management, maintenance, support and Documentation of the ICT Environments, underlying infrastructure, computing platforms, processes and personnel supporting the centrally delivered Business Applications;
		4.1.4 Providing Hosting Services to enable the delivery of End to End Services and FITS Services for both Live Environments and Non-Live Environments;
		4.1.5 Providing Business As Usual support for all business as usual service management functions;
		4.1.6 Providing programme, project and security management services for the elements of the Hosting Service that are within the Hosting Supplier's scope;
		4.1.7 Undertaking pro-active and corrective maintenance for Hosting Services, ensuring that all events, incidents and problems are resolved;
		4.1.8 Providing Gateway Services for secure access to the Authority's Services;
		4.1.9 Providing assurance to the Authority of the Hosting Supplier's capability to deliver shared services to multiple customers without impacting the Authority's Services, Standards, Service Level Targets and Security requirements; and

Requirement No.	Level	Requirement
		4.1.10 Ensuring the Authority's Services, Standards, Service Level Targets and Security requirements are met.
		4.2 The Hosting Supplier shall comply with the obligations on the Hosting Supplier set out in Annex 1.
		5. STRUCTURE OF HOSTING REQUIREMENTS
		5.1 The Hosting Supplier requirements are described in terms of a number of levels specified at level 0, 1, 2 and 3.
		5.1.1 Level 0 refers to the highest level of category (e.g. ITIL service practice). Levels 1 (L1) are the Service Lines and level 2 (L2) are process or function requirement headings of FITS Services to be provided (e.g. level 1: Availability Management; level 2: Plan and Design Availability);
		5.1.2 Level 3 (L3) are the required obligations for each level 1 (category) and level 2 (sub category);
		5.1.3 All level 3 obligations are set out in the tables and contain a unique reference number.
		5.1.4 The Hosting Supplier shall perform all level 3 obligations.
		6. GENERAL PRINCIPLES
		6.1 Within the requirements set out for the Hosting Supplier, certain principles apply with regards to the obligations on the Hosting Supplier, Other FITS Suppliers, Collaborating Suppliers and the Authority.
		6.2 The Authority shall provide the Service Strategy detailing the required business outcomes, preferences and attributes and expectations for all FITS Services.

Requirement No.	Level	Requirement
		6.3 The Hosting Supplier shall identify in schedule 3.2 (Other Service Tower Responsibilities) all Dependencies on the Suppliers necessary for the successful delivery of the Hosting Services under this Agreement including the development of and compliance with any Policies, Processes and Procedures for which the Hosting Supplier is responsible.
		6.4 All Hosting Services shall include Documentation including, but not limited to, Policies, Procedures, Processes, Product Descriptions, detailed operational documentation, technical documentation and operational diagrams and workflows.
		6.5 The Data Centre Service shall be provided by a separate Collaborating Supplier.
		6.6 The SIAM Supplier shall provide and maintain all ITIL and Service Management Policies, Processes and Procedures. The Hosting Supplier shall support the SIAM Supplier where required by providing material to the SIAM Supplier where content has been created or maintained in support of the Hosting Service.
		6.7 The Other FITS Suppliers and Collaborating Suppliers shall be responsible for the production, management and maintenance of their own operational Processes and Procedures and shall ensure that the up to date operational Processes and Procedures are provided to the Hosting Supplier via the SKMS.
		6.8 The Authority shall review and decide Approval of the Policies, Processes and Procedures provided by the Hosting Supplier and will comply with these once agreed.
		6.9 The SIAM Supplier will monitor the compliance and address any non-compliance of the Suppliers and the Authority to the agreed Policies, Processes and Procedures provided by the SIAM Supplier.
		7. FITS STRATEGIC DESIGN THEMES
		7.1 The Authority has developed a number of themes which are at the core of its thinking in the design of the FITS Programme, the TOM and the FITS Services to be provided therein.

Requirement No.	Level	Requirement
		7.2 Providing a consistent user experience: Enables End Users to access their Business Applications and other ICT services from the most appropriate devices for their work setting, and from any Authority location. As End Users move between different locations, including both Authority Sites and remote locations, their experience of their ICT services remains consistent, supporting more flexible accommodation and cross-functional work patterns. An increasing number of Business Applications and services can be securely accessed from non-Authority devices, supporting the increasing participation of other Agencies and the private sector in Authority business activities. End Users are encouraged to use self service facilities for everyday activities such as maintaining personal information, requesting new services and checking on service health. End Users have a single point of contact for all issues around ICT service through a one stop Service Desk, ensuring that their issues are effectively progressed and resolved, and provide realistic expectations of the impact of planned changes and unplanned events.
		7.3 Delivering better for less: FITS Service performance and availability are monitored from business identified transactions and major service consumption points. Service performance and recent historical levels are available from each Supplier. Incidents that threaten business service levels are rapidly and accurately diagnosed and mitigated – with Suppliers incentivised to work together irrespective of where the cause lies. A unified security management regime ensures that information risks are identified, managed appropriately. Suppliers are encouraged to bring innovation relevant to the Authority that may result in improved value for money through the adoption of new technology and the more efficient use of existing resources. Suppliers are working in partnership, to improve service offerings and reduce costs to the Authority. As End User populations and business volumes change, FITS Services are provided in line with the business capacity forecast. Resources and services are regarded 'as a Service' to ensure that predictable pricing models are used and improved budgeting can be implemented.

Requirement No.	Level	Requirement
		7.4 Enabling business transformation: The Authority can take advantage of consistent, and strategically aligned, FITS Services to drive efficiencies in their day to day business. Better interoperation across the Authority is enabling an increase in the use of video conferencing for hearings and meetings; increasing productivity and reducing security and transport costs. Common telephony, voice mail, instant messaging and document sharing facilities are improving the ability of the Authority to manage and communicate; and to explore and adopt new ways of working. The ability to access Business Applications and FITS Services from any Authority Site enables End Users to work flexibly and common business functions to be regrouped or devolved as needed to gain efficiencies. Throughout the change lifecycle, the Authority's information assurance functions works in tandem with the FITS Suppliers to ensure data confidentiality, integrity and availability is maintained - by completing thorough risk assessments and implementing a standard set of comprehensive controls, appropriate to the changes taking place.
		7.5 Aligned with financial governance: The Authority is paying for the FITS Services that it consumes, with usage information and costs available on a timely basis and presented in a form that is transparent and supports decision making in the business. A clear linkage can be established between FITS Service consumption and spend, incentivising the Authority to optimise utilisation of FITS Services and reduce any over-capacity. ICT costs are controlled and the Authority has sufficient historical and current information to understand financial trends alongside consumption trends for the FITS Services. Retained organisation costs are regularly reviewed to ensure that the retained organisation is optimally organised to deliver End to End Services.
		7.6 Supporting cross-Government agenda: The Authority is involved in shaping and implementing Government ICT ideas, and in some areas is leading on behalf of a broader set of Government agencies. The Authority is taking advantage of commodity connectivity services through PSN and other commodity "cloud" based services available from other Government departments and commercial "cloud" solution providers.

Requirement No.	Level	Requirement
		7.7 Maintaining business continuity through transition: The SIAM Supplier provides the FITS Transition Assurance Function as a central role between the Authority, exiting and new Suppliers. The Hosting Supplier transition plans and activities evolve through careful due diligence, planning and agreement between exiting suppliers, Suppliers and the Authority. Transition risks will be identified, with potential business impacts associated with those risks having been understood and appropriate contingency measures to mitigate them having been put in place. The potential impact of transition on the Authority needs to be carefully researched, planned and executed and any transition activities will be agreed with the Authority. As the transition progresses, the new FITS FMO processes will be implemented and matured. Where existing suppliers have had longer run-off obligations, their service and delivery models have been adapted, by Authority agreement, to work effectively within the new operating model.
		8. FITS TOM DESIGN PRINCIPLES FOR HOSTING SERVICES
		8.1 The overarching design aim for the Hosting Supplier is to create standard, consistent and integrated services, with industrialised delivery methodologies that maximise business benefit and minimise business disruption.
		8.2 Implement the Hosting Service components of the FITS Services in a modular, commoditised, flexible and scalable manner.
		8.3 Facilitate process efficiency by choosing automation over manual intervention and empowering the business to self-serve.
		8.4 Design the hosting infrastructure and the associated systems by maximising the contribution to the Greening Government initiative whilst minimising environmental impact.
		8.5 Ensure that the business, its processes, and objectives are understood and considered when designing and delivering Hosting Services to maximise alignment and implementation of business strategy.
		8.6 Deliver a cost-efficient Hosting Service and that meets Service Level Targets, Standards and IA requirements.

Requirement No.	Level	Requirement
		9. HOSTING SERVICE REQUIREMENTS
		9.1 Potential Providers should note that where L2 headings are used in the explanation of the L3 requirements, it is not the intention to observe these as defined terms as set out in schedule 1.
		9.2 Unless otherwise stated, all L3 requirements are within scope of the Hosting Services and are mandatory in delivery of the Hosting Services.
		9.3 To assist Potential Suppliers, each L1 has a description of the types of service the Authority expects to be delivered within the L1 section. These are not commercially binding, but added to provide support and clarity to Suppliers and will be removed from the final document. The L2 and L3 requirements form the commercial scope for Hosting Services.
		9.4 Words which have been capitalised within schedule 2.1 are described as defined terms and their definitions are contained within schedule 1 (Definitions) or are standard ITIL terms.
		10. GENERAL REQUIREMENTS
		10.1 General Principles
		10.1.1 General Principles against which the Hosting Services Service Requirements are to be delivered are listed below:
	2	**General Principles**
01-0-0-001-03 (Common)	3	Not used
01-0-0-002-03 (Common)	3	Not used

Requirement No.	Level	Requirement
01-0-0-003-03 (Common)	3	The Hosting Supplier shall annually self-assess the maturity of the Hosting Services using the HMG Green ICT Maturity Assessment Model and provide the findings to the Authority within thirty (30) Working Days of the anniversary of the Effective Date.
01-0-0-004-01	3	Not used
01-0-0-004-03 (Common)	3	Not used
01-0-0-005-03	3	The Hosting Supplier shall deliver a Hosting Service that complies with all HMG Policies and Strategies and those Strategies and Standards set out in schedule 2.3 (Standards).
01-0-0-006-03	3	NOT USED
01-0-0-007-03	3	NOT USED
01-0-0-008-03	3	NOT USED
01-0-0-011-03	3	The Hosting Supplier shall provide Hosting Services that are provisioned with the capability to leverage environments, infrastructure, network, Platform and other Hosting Services for Multi-Tenanted use in accordance with schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan).
01-0-0-012-03	3	Not used
01-0-0-013-03	3	Not used
01-0-0-014-03	3	The Hosting Supplier shall proactively seek to identify opportunities to provide Hosting Services more efficiently and at a lower cost to the Authority.

Requirement No.	Level	Requirement
01-0-0-015-01	3	The Hosting Supplier shall provide to the SIAM Supplier for inclusion in the Configuration Management System and within six (6) months of the Effective Date, Documentation in support of the delivery, management and maintenance of the Hosting Services described in this schedule. This shall include, but not be limited to: (i) High level designs; (ii) Low level designs; (iii) Service architectures; (iv) Service support work procedures and/or instructions; (v) Support documentation; (vi) Functional specifications; (vii) Technology roadmaps for hardware and software deployed to deliver the Print Services; (viii) Data architectures; and (ix) Training material.
01-0-0-015-03	3	NOT USED
01-0-0-016-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Policies, Processes and Procedures and implement any required corrective action that has been Approved.
01-0-0-016-03	3	The Hosting Supplier shall provide, support and maintain Hosting Services in accordance with the requirements as defined in schedule 2.2 (Service Performance Management), schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan).

Requirement No.	Level	Requirement
01-0-0-017-01	3	The Hosting Supplier shall comply with and assist in audits of Documentation quality where requested by the SIAM Supplier or the Authority.
01-0-0-017-03	3	NOT USED
01-0-0-018-01	3	The Hosting Supplier shall comply with the Polices, Processes and Procedures as defined by the SIAM Supplier.
01-0-0-018-03 (Common)	3	The Hosting Supplier shall consider the use of Open Source Software in accordance with the Cabinet Office's Open Source Procurement Toolkit in the delivery of the Hosting Services. The Hosting Supplier shall make available via the SKMS, a report demonstrating their conformance with the Cabinet Office's 'Assessment of Software for Government' model on an annual basis following the Effective Date.
01-0-0-019-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier as required in defining the SIAM Supplier's Policies, Processes and Procedures for FITS Services.
01-0-0-019-03 (Common)	3	The Hosting Supplier shall, unless otherwise agreed with the Authority, ensure that all solutions and solution components shall meet the functional needs of the Authority and comply with Open Standards where they exist.
01-0-0-020-01	3	The Hosting Supplier shall provide and maintain Approved documentation for inclusion in the SIAM Supplier's SKMS.
01-0-0-020-03 (Common)	3	. Not used
01-0-0-021-03 (Common)	3	Not used
01-0-0-022-03 (Common)	3	Not used

Requirement No.	Level	Requirement
		11. SERVICE STRATEGY
		11.1 Demand Management
		11.1.1 Demand Management is a critical activity within Service Management. Demand Management aims to manage the uncertainty in business demand for FITS Services and ensure the appropriate Capacity of a FITS Service is available as and when required by the Authority.
		11.1.2 The Demand Management process aims to understand the Authority's consumption levels for FITS Services and how these vary over the business cycle, with the aim of ensuring the provision of an appropriate level of service to support the Authority's need.
		11.1.3 The benefit of effective Demand Management is:
		(a) The design for services is optimised to meet the Patterns of Business Activity (PBA) they support;
		(b) Effective management of the FITS Service Catalogue by mapping demand to appropriate FITS Services;
		(c) Informs investment decisions in the management of the Service Portfolio; and
		(d) Informs resource scheduling and management.
		11.1.4 The Service Requirements for Demand Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
02-01-01-001-03	3	NOT USED
02-01-01-002-03	3	NOT USED
02-01-01-003-03	3	NOT USED
02-01-01-004-03	3	NOT USED
02-01-01-005-03	3	NOT USED
02-01-01-006-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Demand Management System; or (ii) Implement a Demand Management System that supports the SIAM Supplier's Demand Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Demand Management System.
02-01-01-007-01	3	The Hosting Supplier shall at all times comply with the SIAM Supplier's Demand Management Policies, Processes and Procedures.
02-01-01-012-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Demand Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
02-01-01-014-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Demand Management Policies, Processes and Procedures.
02-01-01-015-01	3	The Hosting Supplier shall provide Demand Management for Hosting Services in accordance with the SIAM Supplier's Demand Management Policies, Processes and Procedures.
	2	**Analyse and Understand Patterns of Business Activity**

Requirement No.	Level	Requirement
02-01-02-004-01	3	The Hosting Supplier shall support the SIAM Supplier in performing service activity based analysis.
	2	**Define, Match and Report on User Profiles**
02-01-03-003-01	3	The Hosting Supplier shall support the SIAM Supplier to compile Hosting Service forecasts for each Service Reporting Period.
	2	**Develop Service Packages**
02-01-04-002-01	3	The Hosting Supplier shall support the SIAM Supplier in making recommendations on changes or improvements to the composition of Service Package for Hosting Services, including appropriate Service Levels.

Requirement No.	Level	Requirement
		11.2 Financial Management
		11.2.1 The Financial Management process shall provide the Authority with the quantification of the value of all FITS Services provided by the Suppliers and consumed by the Authority in financial terms.
		11.2.2 The Financial Management service is required to ensure that the Authority only pays for the FITS Services it consumes or is obligated to pay for in line with appropriate commercial agreements.
		The benefit of Financial Management is that it helps and supports the Authority in being able to:
		(a) Inform decision making to enable the achievement of stated ICT 'run and maintain' savings;
		(b) Determine the size, scope and complexity of the Service Portfolio;
		(c) Ensures financial compliance and control;
		(d) Apportion charges appropriately;
		(e) Maintain operational cost control; and
		(f) Conduct service lifecycle investment analysis.
		11.2.3 The Service Requirements for Financial Management are listed below:
	2	**General Requirements**
02-02-01-001-03	3	The Hosting Supplier shall provide Financial Management for Hosting Services in accordance with the Authority's Financial Management Policies, Processes and Procedures.
02-02-01-002-03	3	NOT USED

Requirement No.	Level	Requirement
02-02-01-003-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Financial Management System; or (ii) Implement a Financial Management System that supports the Authority's Financial Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Financial Management System.
02-02-01-004-01	3	The Hosting Supplier shall comply with the Authority's Financial Management Policies, Processes and Procedures.
02-02-01-005-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the Authority's Financial Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
	2	**Validate Service Consumption**
02-02-02-003-01	3	Not used
02-02-02-004-01	3	Not used
02-02-02-006-01	3	Not used
	2	**Forecasting and Business Case Support**
02-02-03-003-01	3	The Hosting Supplier shall provide relevant financial information in a timely manner to input into detailed Business Cases for Changes to FITS Services.
02-02-03-005-01	3	The Hosting Supplier shall support the SIAM Supplier with financial forecasting in respect of the FITS Services in support of the Authority's budgeting process.

Requirement No.	Level	Requirement
	2	**Request to Pay**
02-02-04-003-01	3	Not used
		11.3 Service Portfolio Management
		11.3.1 Service Portfolio Management is the process responsible for managing the Service Portfolio and ensuring that business value is achieved across all FITS Services provided to the Authority.
		11.3.2 Service Portfolio Management provides the overall governance in the identification, provision of, delivery and retirement of FITS Services provided by the FITS Suppliers. The Hosting Supplier will work with the Authority and the SIAM provider in providing the Service Portfolio service and will identify and present to the Authority suggestions for the aggregation, improvement, refresh and retirement of FITS Services.
		11.3.3 The benefit of Service Portfolio Management to the Authority is demonstrated through the ability to anticipate change while maintaining traceability to the Authority's overarching ICT strategy and planning by:
		(a) Providing the means to characterise service investments; and
		(b) Providing an essential link between business portfolio management (demand pipeline) and IT project and programme portfolio management.
		11.3.4 The Service Requirements for Service Portfolio Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
02-03-01-001-03	3	NOT USED
02-03-01-002-03	3	NOT USED
02-03-01-003-03	3	NOT USED
02-03-01-004-03	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Service Portfolio Management Policies, Processes and Procedures.
02-03-01-005-03	3	NOT USED
02-03-01-006-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Service Portfolio Management System; or (ii) Implement a Service Portfolio Management System that supports the SIAM Supplier's Service Portfolio Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Service Portfolio Management System.
02-03-01-007-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Portfolio Policies, Processes and Procedures.
02-03-01-008-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Service Portfolio Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
02-03-01-009-01	3	The Hosting Supplier shall provide Service Portfolio Management for Hosting Services in accordance with the SIAM Supplier's Service Portfolio Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
02-03-01-010-01	3	The Hosting Supplier shall, upon commissioning new Hosting Services, document the new Hosting Service and publish in the SIAM Supplier's SKMS within one (1) Month.
	2	**Define the Cross Tower Service Portfolio**
02-03-02-002-01	3	The Hosting Supplier shall produce, maintain and provide to the SIAM Supplier details of the Service Portfolio for the Hosting Services they provide.

Requirement No.	Level	Requirement
		11.4 Risk Management
		11.4.1 The Risk Management process needs to be aligned with the Authority's strategic risk management approach and contain the following steps across the Service Delivery Lifecycle.
		(a) Identification and assessment of exposure to risk and subsequent impacts;
		(b) Application of appropriate controls to manage exposure and impact;
		(c) Ensure communication of mitigating actions; and
		(d) Management of risk is performed within a transparent, repeatable and consistent process.
		11.4.2 Risk Management supports the decision making process by being able to accurately assess risks and the associated impacts and potential benefits of actions in relation to the ability to support and deliver FITS Services.
		11.4.3 Effective Risk Management enables the identification of positive and negative risks to be analysed and a course of action to be determined based on value and impact to the Service Delivery Lifecycle, ensuring that the best possible outcome can be achieved.
		11.4.4 The Service Requirements for Risk Management are listed below:
	2	**General Requirements**
02-04-01-001-03	3	NOT USED

Requirement No.	Level	Requirement
02-04-01-002-03	3	NOT USED
02-04-01-003-03	3	NOT USED
02-04-01-004-03	3	NOT USED
02-04-01-005-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Risk Management System; or (ii) Implement a Risk Management System that supports the SIAM Supplier's Risk Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Risk Management System.
02-04-01-007-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Risk Management Policies, Processes and Procedures.
02-04-01-012-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Risk Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
02-04-01-013-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Risk Management Policies, Processes and Procedures.
02-04-01-014-01	3	The Hosting Supplier shall provide Risk Management for Hosting Services in accordance with the SIAM Supplier's Risk Management Policies, Processes and Procedures.
	2	**Risk Identification and Capture**

Requirement No.	Level	Requirement
02-04-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the identification, analysis and management of risks across the Service Delivery Lifecycle in accordance with the SIAM Supplier's Risk Management Policies, Processes and Procedures.
02-04-02-005-01	3	The Hosting Supplier shall support the SIAM Supplier in making Risk Management information available to the Authority.
	2	**Risk Monitoring**
02-04-03-002-01	3	The Hosting Supplier shall conduct proactive monitoring to identify any emergent risk to the provision of FITS Services and where possible End to End Services and report these immediately to the SIAM Supplier.
	2	**Risk Reporting**
02-04-04-003-01	3	The Hosting Supplier shall attend risk review boards, develop and manage risk action plans and recommend to the SIAM Supplier appropriate measures to mitigate any risk identified.
02-04-04-007-01	3	Where requested by the SIAM Supplier, the Hosting Supplier shall implement the measures identified in answer to an emerging risk which has been Approved by the Authority within twenty (20) Working Days of Approval being granted.

Requirement No.	Level	Requirement
		12. SERVICE DESIGN
		12.1 The purpose of the Service Design phase is to ensure that the design and development of FITS Services, both new and existing, deliver value to the Authority
		12.2 Availability Management
		12.2.1 The service should include the following steps in the Availability Management lifecycle:
		(a) Design for availability;
		(b) Monitor, measure and report availability; and
		(c) Manage risk to availability.
		12.2.2 The purpose of Availability Management is to define, analyse, plan, measure and improve all aspects of the availability of the Hosting Supplier's ICT environments and services. Availability Management is responsible for ensuring that all Hosting Service IT infrastructures, processes, tools and resources are appropriate for the agreed availability targets.
		12.2.3 The benefit of Availability Management is that the process ensures that the availability of systems and services matches the evolving agreed needs of the business. The availability and reliability of ICT environments, systems and services can directly influence customer satisfaction and the reputation of the business.
		12.2.4 The Service Requirements for Availability Management are listed below:

Requirement No.	Level	Requirement
	2	**General Requirements**
03-01-01-001-03	3	The Hosting Supplier shall provide Hosting Services that comply with the applicable Service Levels in accordance with requirements defined in schedule 2.2 (Service Performance Management).
03-01-01-002-03	3	NOT USED
03-01-01-003-03	3	NOT USED
03-01-01-005-03	3	NOT USED
03-01-01-006-03	3	NOT USED
03-01-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Availability Management Policies, Processes and Procedures.
03-01-01-015-01	3	The Hosting Supplier shall ensure that any AMIS that they use interfaces effectively with the cross tower AMIS provided by the SIAM Supplier in accordance with the SIAM Supplier's Availability Management Policies Processes and Procedures.
03-01-01-016-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Availability Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
03-01-01-017-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Availability Management Policies, Processes and Procedures.
03-01-01-018-01	3	The Hosting Supplier shall provide Availability Management for Hosting Services in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures.
	2	**Plan and Design Availability**

Requirement No.	Level	Requirement
03-01-02-001-03	3	The Hosting Supplier shall provide and deliver the Hosting Services to the Authority Service Levels, or propose alternatives for Authority Approval, for Future Services or changed Hosting Services in accordance with the Change Control Process.
03-01-02-003-01	3	The Hosting Supplier shall provide and deliver the Hosting Services to the agreed availability, design criteria and Service Levels for Future Services or changed Hosting Services in accordance with the Change Control Process.
03-01-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier in producing and updating the Availability Plan every Service Reporting Period in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures.
	2	**Assess and Manage Risk to Availability**
03-01-03-002-01	3	The Hosting Supplier shall actively participate in availability risk reviews carried out on the FITS Services by the SIAM Supplier.
	2	**Monitor, Measure, Analyse, Report, and Review Availability**
03-01-04-002-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures to schedule and manage any Planned Outages in order to minimise disruption to normal business operations
03-01-04-005-01	3	The Hosting Supplier shall provide to the SIAM Supplier the Projected Service Outage information in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures.
03-01-04-011-01	3	The Hosting Supplier shall provide Availability data to the SIAM Suppliers via the Availability Management and Information System in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures.
03-01-04-014-01	3	The Hosting Supplier shall gather and deliver to the SIAM Supplier the data as defined in the SIAM Supplier's Availability Management Policies, Processes and Procedures

Requirement No.	Level	Requirement
	2	**Investigate and Implement Measures to Improve Availability Performance**
03-01-05-002-01	3	The Hosting Supplier shall produce for the SIAM Supplier Component Failure Impact Analysis information within each Service Measurement Period in accordance with the SIAM Supplier's Availability Management Policies, Processes and Procedures and propose to the SIAM Supplier possible mitigation actions to avoid future degradation of the availability of Hosting Services or components thereof.
		12.3 Capacity Management
		12.3.1 The service should provide the following sub processes within the Capacity Management Lifecycle:
		(a) Hosting Service Capacity Management;
		(b) Hosting Service Capacity Management reporting.
		12.3.2 The purpose of Capacity Management is to ensure that the capacity of FITS Services and the supporting ICT environment and services is able to deliver the agreed Service Levels, Service Level Targets and Key Performance Indicators in an efficient and timely manner.
		12.3.3 The benefit of Capacity Management is that it is responsible for ensuring that resources are planned and scheduled to provide a consistent level of service that is matched to the current and future needs of the Authority. Capacity Management provides a Capacity Plan that outlines the resources needed to support the required business outcomes.
		12.3.4 The Service Requirements for Capacity Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
03-02-01-001-03	3	NOT USED
03-02-01-002-03	3	NOT USED
03-02-01-004-03	3	NOT USED
03-02-01-005-03	3	NOT USED
03-02-01-006-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Capacity Management System; or (ii) Implement a Capacity Management System that supports the SIAM Supplier's Capacity Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Capacity Management System.
03-02-01-007-03	3	NOT USED
03-02-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Capacity Management Policies, Processes and Procedures.
03-02-01-015-01	3	The Hosting Supplier shall support the SIAM Supplier in the production and maintenance of a FITS Capacity Plan by providing the SIAM Supplier with Capacity Plans for the FITS Services and components thereof they are providing.
03-02-01-018-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.

Requirement No.	Level	Requirement
03-02-01-019-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in the production, maintenance, review and subsequent implementation of any agreed corrective action(s) to the Capacity Plan(s), in accordance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures.
03-02-01-020-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Capacity Management Policies, Processes and Procedures.
03-02-01-021-01	3	The Hosting Supplier shall provide Capacity Management for Hosting Services in accordance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures.
	2	**Review Current Capacity**
03-02-02-008-01	3	Following receipt of the Quarterly Business Forecast from the SIAM Supplier, and in accordance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures, the Hosting Supplier shall: (i) Update their respective Capacity Plan to include those future volumes; and (ii) Submit their Capacity Plan to the SIAM Supplier.
03-02-02-010-01	3	The Hosting Supplier shall provide Capacity information required by the SIAM Supplier for inclusion into the FITS CMIS.
	2	**Assess and Document Capacity Requirements**
03-02-03-003-01	3	The Hosting Supplier shall support the SIAM Supplier to model any proposed Change and the consumption trends in the FITS Services in order to identify any Change that needs to be made to current Hosting Services or components thereof to ensure that the Service Levels are achieved.
03-02-03-006-01	3	The Hosting Supplier shall manage the availability of appropriate resources units to meet the predicted demands to the Hosting Services.

Requirement No.	Level	Requirement
03-02-03-008-01	3	The Hosting Supplier shall support the SIAM Supplier in monitoring the Hosting Services against the agreed Capacity thresholds.
03-02-03-010-01	3	The Hosting Supplier shall monitor the Hosting Services for which they are responsible, as agreed with the Authority against the agreed Capacity thresholds and notify the SIAM Supplier as soon as they become aware of any Capacity issues or potential Capacity issues.
03-02-03-012-01	3	The Hosting Supplier shall continually monitor and optimise Capacity by increasing or decreasing Capacity in accordance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures in order for the Hosting Services to maintain the operation of the Hosting Services in accordance with schedule 2.2 (Service Performance Management).
03-02-03-013-01	3	The Hosting Supplier shall produce and submit a Capacity Report for the FITS Services they are providing to the SIAM Supplier in accordance with the SIAM Supplier's Capacity Management Policies, Processes and Procedures for each Service Reporting Period comparing the actual volumes provided against the volumes forecasted in their Capacity Plan.
03-02-03-016-01	3	The Hosting Supplier shall produce and submit to the SIAM Supplier a Quarterly Capacity Plan as advised by the SIAM Supplier and in accordance with the SIAM Supplier's Capacity Management Policies and Procedures

Requirement No.	Level	Requirement
		12.4 IT Service Continuity Management
		12.4.1 IT Service Continuity Management (ITSCM) shall support the overall Authority's Business Continuity Management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required and agreed business timescales. 12.4.2 The ITSCM Services documented in paragraph 12.4 relate only to the role undertaken by the Hosting Supplier, whether a test or service operation, and are limited to establishing available hosting services where practicable at the secondary site. The Hosting Supplier cannot guarantee or warrant the functionality of the Business Applications in the event of an ITSCM event, including but not limited to a Disaster Recovery event (whether a test or service operation) as this is beyond the scope of the Hosting Services
		12.4.3 ITSCM shall support the Authority's Business Continuity planning process and ensure that the recovery arrangements for designated FITS Services and components thereof are aligned to identified and agreed business impacts, risks and needs.
		12.4.4 ITSCM manages the risks that could materially impact the performance and availability of the FITS Services as part of the End to End Services. ITSCM ensures that FITS Services can be provided in accordance with agreed Service Levels.
		12.4.5 The Service Requirements for IT Service Continuity Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
03-03-01-001-03	3	NOT USED
03-03-01-002-03	3	NOT USED
03-03-01-003-03	3	NOT USED
03-03-01-004-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's ITSC Management System; or (ii) Implement an ITSC Management System that supports the SIAM Supplier's ITSC Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's ITSC Management System.
03-03-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's ITSC Management Policies, Processes and Procedures.
03-03-01-017-01	3	The Hosting Supplier shall provide the SIAM Supplier with a SPoC for the ITSCM Plan and provide an escalation process with full contact details. The SPoC shall be identified as a Key Personnel as set out in schedule 9.2 (Key Personnel).
03-03-01-022-01	3	The Hosting Supplier shall support the ITSCM planning process ensuring its ITSCM Plan aligns to the SIAM Supplier's ITSCM Plan.
03-03-01-025-01	3	The Hosting Supplier shall develop and maintain an up-to-date ITSCM Plan for the Hosting Services they provide that is consistent and conformant with the SIAM Suppliers ITSCM Plan, and provide a copy of its ITSCM Plan to the SIAM Supplier in accordance with the ITSCM Policies, Processes and Procedures
03-03-01-028-01	3	The Hosting Supplier shall provide ITSC Awareness Training for all their ITSCM related personnel within three (3) months of the Effective Date.

Requirement No.	Level	Requirement
03-03-01-029-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's ITSCM Policies, Processes and Procedures and implement any required corrective action that has been Approved.
03-03-01-030-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's ITSCM Policies, Processes and Procedures.
03-03-01-031-01	3	The Hosting Supplier shall provide ITSCM for Hosting Services in accordance with the SIAM Supplier's ITSC Management Policies, Processes and Procedures.
	2	**Determine Requirements for ITSC Plans**
03-03-02-005-01	3	The Hosting Supplier shall ensure that all Business Impact Analysis communicated by the SIAM Supplier are factored into their ITSC Plan(s) for the Hosting Services.
03-03-02-008-01	3	The Hosting Supplier shall support the SIAM Supplier in undertaking an annual review, or a review post invocation, of the ITSCM Plan and associated processes.
	2	**Make Updates to the ITSCM Plan**
	3	Not applicable
	2	**ITSCM Testing**
03-03-04-001-03	3	NOT USED
03-03-04-003-01	3	The Hosting Supplier shall participate in the ITSCM Test exercise regime and undertake the relevant activities in compliance with the ITSCM Testing Schedule.
03-03-04-007-01	3	The Hosting Supplier shall review the draft ITSCM Test Schedule provided by the SIAM Supplier and shall submit information and assistance as required by the SIAM Supplier.

Requirement No.	Level	Requirement
03-03-04-008-01	3	The Hosting Supplier shall comply with the ITSCM Test Schedule and the ITSC Management Policies and Procedures at all times
03-03-04-009-01	3	The Hosting Supplier shall, when they have executed tests defined under the ITSCM Test Schedule for the FITS Services they provide the SIAM Supplier with the appropriate ITSCM Test Reports and remediation plans including a possible retest to resolve failed tests in accordance with the ITSCM Policies, Processes and Procedures.
03-03-04-011-01	3	The Hosting Supplier shall support the SIAM Supplier in the planning, implementation, execution and closure of ITSC test events in accordance with the SIAM Supplier's ITSCM Testing Schedule and the SIAM Supplier's ITSCM Policies, Processes and Procedures.
	2	**ITSCM Plan Invocation**
03-03-05-001-03	3	The Hosting Supplier shall, on notification of an ITSC Event, provide information, guidance and assistance in the SIAM Supplier's planning of actions required to restore normal Service.
03-03-05-002-03	3	NOT USED
03-03-05-003-01	3	The Hosting Supplier shall define with the SIAM Supplier clear and unambiguous triggers and closure points relating to ITSC Events.
03-03-05-005-01	3	The Hosting Supplier shall notify the SIAM Supplier of the occurrence of any ITSC Event and shall provide formal recommendations for invoking the relevant ITSC Plan(s) to ensure that Hosting Services are delivered with the agreed recovery objectives and in accordance with schedule 2.2 (Service Performance Management).
03-03-05-009-01	3	Following notice from the SIAM Supplier that it requires an ITSC Plan(s) to be invoked, the Hosting Supplier shall comply and immediately launch the applicable ITSC Plan(s).
03-03-05-012-01	3	Following the agreed closure of an ITSC Event, the Hosting Supplier shall provide the SIAM Supplier with such information, guidance and assistance as may be reasonably requested by the SIAM Supplier to support in the production of the ITSC Event Report.

Requirement No.	Level	Requirement
	2	**ITSCM Reviews**
03-03-06-001-03	3	NOT USED
03-03-06-002-01	3	The Hosting Supplier shall support the SIAM Supplier in ensuring there is appropriate monitoring and review of the ITSCM Plans in accordance with the ITSC Management Policies and Procedures.
03-03-06-004-01	3	The Hosting Supplier shall proactively monitor the Hosting Services, report and propose actions, as soon as is reasonably practical, to the SIAM Supplier on identified emerging risks to the continuity of the provision of the Hosting Services.

Requirement No.	Level	Requirement
		12.5 Service Catalogue Management
		12.5.1 Service Catalogue Management provides a single source of consistent information on all the FITS Services.
		12.5.2 The Service Catalogue Management process shall ensure that the Authority has an accurate Service Catalogue produced and maintained, for all operational services and those being prepared to be run operationally from across the FITS Suppliers.
		12.5.3 Service Catalogue Management shall provide a central source of information on the FITS Services delivered by all FITS Suppliers. The catalogue shall monitor that all areas of the business can view an accurate, consistent picture of all the FITS Services available. It shall contain both an outwardly customer-facing view of the FITS Services available and an internal ICT delivery facing view. Views shall need to be created that show how FITS Services are consumed, the business processes they enable, and the levels and quality of service that can be expected.
		12.5.4 The Service Requirements for Service Catalogue Management are listed below:
	2	**General Requirements**
03-04-01-001-03	3	NOT USED
03-04-01-002-03	3	NOT USED
03-04-01-003-03	3	NOT USED

Requirement No.	Level	Requirement
03-04-01-004-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Service Catalogue Management System; or (ii) Implement a Service Catalogue Management System that supports the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Service Catalogue Management System.
03-04-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures.
03-04-01-014-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
03-04-01-015-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures.
03-04-01-016-01	3	The Hosting Supplier shall provide Service Catalogue Management for Hosting Services in accordance with the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures.
	2	**Agree Service Content and Definition**
03-04-02-002-01	3	The Hosting Supplier shall update and contribute to the production of the FITS Service Catalogue.
	2	**Manage and Maintain the Service Catalogue**
03-04-03-001-03	3	NOT USED

Requirement No.	Level	Requirement
03-04-03-002-01	3	The Hosting Supplier shall maintain their elements of the FITS Service Catalogue in accordance with the SIAM Supplier's Service Portfolio Management, Change and Evaluation Management and Request Fulfilment Policies, Processes and Procedures to ensure that they are always current with the FITS Services.
03-04-03-007-01	3	The Hosting Supplier shall support the development and maintenance of a subset of the FITS Service Catalogue so that it is available to all Authority End Users.
03-04-03-012-01	3	The Hosting Supplier shall agree and document Service Definitions and all relevant documentation (as detailed in the SIAM Supplier's Service Catalogue Management Policies, Processes and Procedures) with the SIAM Supplier for Hosting Services and components thereof listed in their Service Catalogue.
03-04-03-014-01	3	The Hosting Supplier shall ensure that all Hosting Services and components thereof listed in their Service Catalogue have appropriate Service Assets and Configuration Items (CIs) identified within the Configuration Management System managed by the SIAM Supplier.
03-04-03-017-01	3	The Hosting Supplier shall correct any inaccuracies in the Hosting Supplier's Services, elements or components thereof, within the FITS Service Catalogue that may be identified by the SIAM Supplier in accordance with SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
		12.6 Service Level Management
		12.6.1 The Service Level Management process ensures that the agreed level of service is provided for all FITS Services and that all future FITS Services are delivered to agreed achievable targets. Service Level Management shall demonstrate the following steps within the Service Level Management lifecycle:
		(a) Design and development of Service Levels and Service Level Targets for all FITS Services provided by all FITS Suppliers and Collaborating Suppliers;
		(b) Analyse, determine, document and agree business requirements for a FITS Service and produce and document Service Level Requirements for Approval by the Authority;
		(c) Ensure that appropriate arrangements are agreed and implemented that support the provision of FITS Services to agreed Service Levels, Service Level Targets and Key Performance Indicators and that these are aligned and consistent with those set out in schedule 2.2 (Service Performance Management) and the MSA;
		(d) Implement Service Level Agreements upon Approval;
		(e) Monitor FITS Service performance against Service Level Agreements and produce and communicate regular performance reports; and
		(f) Perform regular FITS Service reviews.
		12.6.2 Service Level Management is a vital process responsible for ensuring that:
		(a) Negotiated and agreed Service Levels for FITS Services from all FITS Suppliers and Collaborating Suppliers are satisfactorily met;

Requirement No.	Level	Requirement
		(b) Back to back arrangements between FITS Suppliers, Collaborating Suppliers and Other Authority Providers and supporting ITSM processes are appropriate and proportionate for the agreed Service Levels;
		(c) Monitoring and reporting on Service Levels is performed; and
		(d) The Authority is regularly informed and engaged on performance of all Service Levels.
		12.6.3 Service Level Management shall provide a consistent interface to the Authority for all FITS Service-related issues. It shall provide the Authority with the agreed Service Levels and the required management information to monitor that those targets have been met. Where targets are breached, Service Level Management should provide feedback on the cause of the breach and details of the actions taken to prevent the breach from reoccurring, thus providing a reliable communication channel and trusted relationship with the Authority representatives.
		12.6.4 The Service Requirements for Service Level Management are listed below:
	2	**General Requirements**
03-05-01-001-03	3	NOT USED
03-05-01-002-03	3	The Hosting Supplier shall ensure that it delivers Hosting Services that are in accordance with the Service Levels as defined in schedule 2.2 (Service Performance Management).
03-05-01-003-03	3	NOT USED
03-05-01-004-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Level Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
03-05-01-004-03	3	NOT USED
03-05-01-005-03	3	NOT USED
03-05-01-006-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Service Level Management System; or (ii) Implement a Service Level Management System that supports the SIAM Supplier's Service Level Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Service Level Management System.
03-05-01-007-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Service Level Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
03-05-01-008-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Service Level Management Policies, Processes and Procedures.
03-05-01-009-01	3	The Hosting Supplier shall provide Service Level Management for Hosting Services in accordance with the SIAM Supplier's Service Level Management Policies, Processes and Procedures.
	2	**Future Services**
03-05-02-002-01	3	The Hosting Supplier shall provide and deliver the FITS Services to the agreed availability, design criteria and Service Levels for Future Services or changed FITS Services in accordance with the Change Control Process.
03-05-02-005-01	3	The Hosting Supplier shall support the SIAM Supplier in managing, monitoring, measuring and reporting on the performance of Hosting Service Levels.

Requirement No.	Level	Requirement
03-05-02-011-01	3	The Hosting Supplier shall support the SIAM Supplier to ensure that all Service Levels are met in accordance with the Service Levels set out in schedule 2.2 (Service Performance Management) and the MSA.
	2	**Document and Agree Service Levels**
	3	Not applicable
	2	**Activate Service Level Agreements**
03-05-04-004-01	3	The Hosting Supplier shall capture, collate and make available to the SIAM Supplier all information relevant to Service Levels for the Hosting Services they provide in accordance with schedule 2.2 (Service Performance Management) and the MSA and to make this information available to the SIAM Supplier both in real time and as per the Service Reporting Period set out in schedule 2.2 (Service Performance Management).
	2	**Agree Reporting Framework**
03-05-05-005-01	3	The Hosting Supplier shall support the SIAM Supplier in the analysis of data in provision of performance measurement information
03-05-05-008-01	3	The Hosting Supplier shall support the SIAM Supplier in reviewing any Service Level Target failures and/or threatened breaches and agree the content of an Exception Report including a proposed approach to resolving such failures for future service operation in accordance with schedule 2.2 (Service Performance Management).
03-05-05-010-01	3	The Hosting Supplier shall support the SIAM Supplier in the development of a Systems of Measurement Reference Document for all Hosting Services that contribute to the Service Levels as specified in schedule 2.2 (Service Performance Management).

Requirement No.	Level	Requirement
03-05-05-013-01	3	The Hosting Supplier shall attend monthly FITS Service reviews managed by the SIAM Supplier at any Authority designated location on request with no less than one (1) week notice, to assess and review performance of FITS Services against performance criteria set out in schedule 2.2 (Service Performance Management) and the MSA.

Requirement No.	Level	Requirement
		12.7 Supplier Management
		12.7.1 The Supplier Management requirements contain the responsibilities of the Hosting Supplier in support of the Authority in the monitoring and reviewing the performance and engagement of all FITS Suppliers in complying with obligations to the Policies and Procedures set down by the SIAM Supplier and their contracted obligations agreed with the Authority.
		12.7.2 The main objectives for the Supplier Management process are:
		(a) Work with Other FITS Suppliers to ensure conformance and adherence to agreed Policies and Procedures;
		(b) Manage the take on of new Suppliers, Other Authority Providers and the Hosting Suppliers sub contractors;
		(c) Manage the non compliance to Policies and Procedures by any Supplier;
		(d) Manage the day-to-day operational relationship with Other FITS Suppliers and Collaborating Suppliers;
		(e) Conduct regular performance reviews with Other FITS Suppliers and Collaborating Suppliers; and
		(f) Provide an interface for formal communications from all Suppliers and the Authority.
		12.7.3 This is a valuable process to the Authority as it ensures that the day to day engagement with the Other FITS Suppliers and Collaborating Suppliers is managed to ensure that all suppliers operate to a common understanding and performance level.

Requirement No.	Level	Requirement
		12.7.4 The Service Requirements for Supplier Management are listed below:
	2	**General Requirements**
03-06-01-001-03	3	The Hosting Supplier shall manage Third Party Software maintenance providers to deliver Workarounds and/or temporary fixes where practicable to the Software until such time as a permanent fix to the Software is made by the Third Party Software maintenance provider.
03-06-01-002-03	3	NOT USED
03-06-01-003-01	3	The Hosting Supplier shall work and collaborate with the Other Suppliers, as identified in the Dependencies Register, to support the SIAM Supplier in delivering the FITS Services in compliance with the Service Levels set out in schedule 2.2 (Service Performance Management) and the Master Services Agreement.
03-06-01-003-03	3	NOT USED
03-06-01-004-03	3	NOT USED
03-06-01-005-03	3	NOT USED
03-06-01-006-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Supplier Management System; or (ii) Implement a Supplier Management System that supports the SIAM Supplier's Supplier Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Supplier Management System.
03-06-01-007-03	3	The Hosting Supplier shall manage Third Party Software Suppliers where they are required to support the delivery of Hosting Services.

Requirement No.	Level	Requirement
03-06-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Supplier Management Policies, Processes and Procedures.
03-06-01-015-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Supplier Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
03-06-01-016-01	3	The Hosting Supplier shall provide Supplier Management for Hosting Services in accordance with the SIAM Supplier's Supplier Management Policies, Processes and Procedures.
03-06-01-017-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Supplier Management Policies, Processes and Procedures.
	2	**Management of the FITS Services Framework**
03-06-02-007-01	3	The Hosting Supplier shall provide all relevant information and support to the SIAM Supplier on FITS Services, agreed standards and performance targets.
03-06-02-011-01	3	The Hosting Supplier shall attend and actively participate in regular Performance Reviews convened by the SIAM Supplier in accordance with the SIAM Supplier's Supplier Management Policies and Procedures..
03-06-02-014-01	3	The Hosting Supplier shall support the SIAM Supplier by attending regular Performance reviews on FITS Services and agreed process improvement plans.
03-06-02-018-01	3	The Hosting Supplier shall support the SIAM Supplier to establish a supplier scorecard.
03-06-02-019-01	3	The Hosting Supplier shall provide appropriate performance information as requested by the SIAM Supplier in support of the production of a regular supplier scorecard.
	2	**Supply Chain Risk Management**

Requirement No.	Level	Requirement
03-06-03-003-01	3	The Hosting Supplier shall support the SIAM Supplier in the management and maintenance of risks to the FITS Service supply chain.
03-06-03-006-01	3	The Hosting Supplier shall participate in and provide support to any review of risks where participation has been requested by the SIAM Supplier or the Authority.

Requirement No.	Level	Requirement
		13. SERVICE TRANSITION
		13.1 Introduction
		The purpose of the Transition phase of the Service Delivery Lifecycle is to plan and coordinate resources to ensure that the requirements derived from the Strategy phase and instilled during the Design phase are effectively realised in Service Operations.
		13.2 Transition Planning and Support
		13.2.1 The Hosting Supplier needs to ensure that the service for the introduction of new or changed FITS Services has the following activities embedded across the Transition Planning and Support lifecycle:
		(a) Develop a strategy for transition;
		(b) Prepare for and plan for transition;
		(c) Ensure Service Design Packages are created for new FITS Services;
		(d) Identify, manage and limit the risks to service interruption;
		(e) Complete Service Requirements capture;
		(f) Complete Service Design;
		(g) Confirm Service Design with the approval body;
		(h) Complete Service Validation Testing;
		(i) Confirm Service Release and Deployment readiness; and

Requirement No.	Level	Requirement
		(j) Perform Service handover and review.
		13.2.2 The main purpose of Transition Planning and Support is to coordinate the resources required to ensure specifications for the design of a new or changed FITS Service are realised. This is achieved through the use of a consistent and repeatable framework for the evaluation of FITS Service capability and risk before a new or changed FITS Service is deployed.
		13.2.3 The benefit of an effective and efficient Transition Planning and Support process is that it enables Projects to estimate and understand costs, timings and resource requirements, with associated risks of transition in to live. This enables:
		(a) Higher volumes of successful Change;
		(b) Improved expectation setting for all Stakeholders;
		(c) Increased confidence in the new or changed FITS Service shall be maintained and supported within a cost-effective manner where there are no unexpected operational costs associated to the live running of the service;
		(d) Better management of the risks in transitioning new FITS Services in to the Authority's ICT Environment;
		(e) Greater alignment between delivery and operational organisations;
		(f) Clear governance over FITS Service Requirements; and
		(g) A reduction in the gap between capability and business requirement.

Requirement No.	Level	Requirement
		13.2.4 The Service Requirements for Transition Planning and Support are listed below:
	2	**Develop Transition Strategy**
04-01-01-002-01	3	The Hosting Supplier shall support the SIAM Supplier, the Authority or its nominated representative in the creation, maintenance and execution of standard, reusable Policies, Procedures and Processes to support a common framework for FITS Service Transition.
	2	**Create Policies and Procedures**
04-01-02-001-03	3	NOT USED
04-01-02-003-01	3	The Hosting Supplier shall comply with the SIAM Supplier's Transition Planning and Support Policies, Processes and Procedures.
04-01-02-006-01	3	The Hosting Supplier shall support all Service Transition activities in accordance with the SIAM Supplier's Transition Planning and Support Processes, Policies and Procedures.
04-01-02-008-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Transition Planning and Support Policies, Processes and Procedures.
	2	**Support to Business Change**
04-01-03-002-01	3	The Hosting Supplier shall on request from the Authority or the SIAM Supplier, support the Authority in the early stage development of the Hosting services aspects of the Proposal Document as defined by the Authority's Integrated ICT lifecycle (stages of Identification, Feasibility and Initiation) in the capture, collation and production of the Proposal Document in support of proposed Business Change.
	2	**Transition Planning**
04-01-04-001-03	3	NOT USED

Requirement No.	Level	Requirement
04-01-04-002-03	3	NOT USED
04-01-04-003-03	3	NOT USED
04-01-04-004-01	3	The Hosting Supplier shall support the SIAM Supplier in the discovery, identification and agreement of Service Requirements to develop a Service Design Package.
04-01-04-004-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Transition Planning and Support System; or (ii) Implement a Transition Planning and Support System that supports the SIAM Supplier's Transition Planning and Support Policies, Processes and Procedures and interfaces with the SIAM Supplier's Transition Planning and Support System.
04-01-04-009-01	3	The Hosting Supplier shall provide details to the SIAM Supplier of the design for new Service Requirements on request from the SIAM Supplier
04-01-04-011-01	3	The Hosting Supplier shall support the SIAM Supplier in the creation of requested Service Design Packages and Transition Models which shall form the basis for all Service Transition. This shall include, but not be limited to: (i) The review of service requirements, Service Transition plans and any associated documentation (ii) Providing resource and delivery time estimates.
04-01-04-014-01	3	The Hosting Supplier shall obtain appropriate approval from the SIAM Supplier for all Service Design Packages before instigating further Service Transition activities.

Requirement No.	Level	Requirement
04-01-04-016-01	3	The Hosting Supplier shall support the SIAM Supplier in ensuring that sufficient and appropriate resources are identified and available to deliver Service Design Packages to time, quality and cost constraints
04-01-04-019-01	3	The Hosting Supplier shall support the SIAM Supplier in ensuring that service risks to failure and disruption across Service Transition have been fully investigated, understood and mitigating actions are in place with appropriate control and management.
04-01-04-021-01	3	The Hosting Supplier shall ensure the completeness and consistency of all inputs/outputs to Service Transition plans they provide to the SIAM Supplier.
04-01-04-022-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Transition Planning and Support Policies, Processes and Procedures and implement any required corrective action that has been Approved.
04-01-04-024-01	3	The Hosting Supplier shall provide Transition Planning and Support for Hosting Services in accordance with the SIAM Supplier's Transition Planning and Support Policies, Processes and Procedures.
	2	**Manage and coordinate Transition**
04-01-05-004-01	3	The Hosting Supplier shall support and participate in Service Design activities as coordinated and directed by the SIAM Supplier.
04-01-05-009-01	3	The Hosting Supplier shall support the SIAM Supplier in the creation of an Early Life Support plan.
04-01-05-014-01	3	The Hosting Supplier shall support the SIAM Supplier and coordinate agreed activities to implement the Approved service delivery and support ITSM processes, tools and governance required to support the introduction of changed FITS Services.
04-01-05-016-01	3	The Hosting Supplier shall ensure that during the course of Service Transition activities the integrity of in situ Service Assets, FITS Services and components thereof and Configurations Items is maintained.

Requirement No.	Level	Requirement
04-01-05-018-01	3	The Hosting Supplier shall support the SIAM Supplier in completing the Service Handover Pack and support in making respective contributions available via the SKMS.
04-01-05-020-01	3	The Hosting Supplier shall support the SIAM Supplier in managing all Service Transition activities in compliance with the Information Security Management process.

Requirement No.	Level	Requirement
		13.3 Change and Evaluation Management
		13.3.1 This service should include the following steps in the Change and Evaluation Management lifecycle:
		(a) Register Requests for Change (RFCs);
		(b) Categorise change;
		(c) Govern Emergency Change;
		(d) Govern Standard (pre-approved) Change;
		(e) Govern Operational Change; and
		(f) Review and close Change.
		13.3.2 The purpose of Change and Evaluation Management is to identify, control and account for Service Assets and Configuration Items (CIs), protecting and ensuring their integrity across the service lifecycle.
		13.3.3 The benefit of effective Change and Evaluation Management to the Authority is that it:
		(a) Prioritises and responds to business driven demand for change to FITS Services;
		(b) Implements changes that meet the Authority's agreed Service Requirements while optimising efficiency;
		(c) Contributes to meeting operational governance, legal, contractual and regulatory requirements;
		(d) Reduces failed changes and service disruption, defects and re-work;

Requirement No.	Level	Requirement
		(e) Delivers change consistently, promptly within expected timescales;
		(f) Contributes to improved estimations of quality, time and cost of change;
		(g) Aids in productivity of resources by minimising disruption due to high levels of unplanned or emergency change thus improving the efficiency and effectiveness of service availability;
		(h) Provides a single tracking facility for all changes through the service lifecycle and to Service Assets;
		(i) Assess the risks associated to the transition of FITS Services, both new and existing; and
		(j) Increases service quality through appropriate Impact Assessment of Changes, thus preventing Incidents.
		13.3.4 The Service Requirements for Change and Evaluation Management are listed below:
	2	**General Requirements**
04-02-01-001-03	3	NOT USED
04-02-01-002-03	3	NOT USED
04-02-01-003-03	3	The Hosting Supplier shall utilise the SIAM Supplier's Change Management System.
04-02-01-004-01	3	The Hosting Supplier shall support and provide input to the SIAM Supplier to develop and maintain the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
04-02-01-007-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier’s Change and Evaluation Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
04-02-01-012-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
04-02-01-013-01	3	The Hosting Supplier shall provide Change Management for Hosting Services in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
	2	**Request for Change Management**
04-02-02-001-01	3	The Hosting Supplier shall raise requests to the SIAM Supplier for Changes including but not limited to: Operational Changes, Standard Changes and Emergency Changes in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
04-02-02-001-03	3	NOT USED
04-02-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier in addressing the governance concerning the raising of Changes by the Authority and the Other Suppliers as identified in the Dependencies Register in accordance with the SIAM Supplier's Change Management Policies, Processes and Procedures.
04-02-02-008-01	3	The Hosting Supplier shall ensure that all Requests for Change they submit contain information including but not limited to: (i) Verified Implementation Plans; (ii) Post Implementation Review; (iii) Acceptance Criteria; (iv) Back Out Plans or Remediation Plans; and (v) Plans for handover to support.

Requirement No.	Level	Requirement
04-02-02-012-01	3	The Hosting Supplier shall ensure that Approved Changes are only implemented by Supplier Personnel or Authorised Representatives in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
04-02-02-014-01	3	The Hosting Supplier shall ensure all Standard Changes employ a consistent way of working and are deployed in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures
04-02-02-017-01	3	The Hosting Supplier shall maintain and provide the SIAM Supplier with a list of nominated Approved Hosting Supplier Personnel who are authorised to request Changes.
04-02-02-019-01	3	The Hosting Supplier shall participate in the activities of the Change Advisory Board (CAB) including but not limited to emergency CAB and the reviews of Requests for Change.
04-02-02-023-01	3	The Hosting Supplier shall support the SIAM Supplier in identifying and developing Standard Changes.
04-02-02-025-01	3	The Hosting Supplier shall provide all information relating to Pre-Approved Changes to the SIAM Supplier for inclusion in the FITS Service Catalogue.
04-02-02-026-01	3	The Hosting Supplier shall inform the SIAM Supplier of all implementations of Pre-Approved Changes.
04-02-02-027-01	3	The Hosting Supplier shall inform the SIAM Supplier of any failure of Pre-Approved Change.
04-02-02-032-01	3	The Hosting Supplier shall receive Change Requests from the SIAM Supplier and will provide an Impact Analysis on such Requests back to the SIAM Supplier for agreement and implementation in accordance with the SIAM Change and Evaluation Management Policies, Processes and Procedures.
	2	**Review, Monitor, Report and Close**
04-02-03-001-03 (Common)	3	The Hosting Supplier shall assess the environmental impact of the introduction of any new Service, or any architecturally significant change to any existing Service, in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
04-02-03-004-01	3	The Hosting Supplier shall provide regular updates to all tasks or activities associated with a Change, where they are responsible for execution, in accordance with the Change and Evaluation Management Policies, Processes and Procedures and support to the SIAM Supplier in presentation of: (i) User views; (ii) ICT views; (iii) Dashboard views; (iv) Business Unit views; and (v) Site views.
04-02-03-007-01	3	The Hosting Supplier shall support the SIAM Supplier in analysing and reporting on the management of Change in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures
04-02-03-009-01	3	The Hosting Supplier shall participate and contribute to Post Implementation Reviews.
04-02-03-013-01	3	The Hosting Supplier shall support the Other Suppliers, as identified in the Dependencies Register, via the SIAM Supplier to ensure that all activities/tasks for a given Change have the appropriate ownership.

Requirement No.	Level	Requirement
		13.4 Knowledge Management
		13.4.1 Knowledge Management is the provision of, and access to, an appropriate store of knowledge and information artefacts relating to the provision, support and maintenance of FITS Services. It enables the provision of quality FITS Services and contribute to the provision of quality End to End Services by ensuring that those responsible for managing the FITS Services and End to End Services are able to do so with access to all current, relevant and appropriate information.
		13.4.2 The purpose of Knowledge Management is to ensure that the right person has the right knowledge at the right time to deliver and support the FITS Services provided to the Authority.
		13.4.3 Knowledge Management is a key service element. Effective Knowledge Management is a powerful asset for people in all roles across all stages of the Service Delivery Lifecycle. It should be the primary method for support individuals and teams to share data, information and knowledge about all facets of service. Knowledge Management needs to include, but is not limited to:
		(a) User profiling and demand characteristics;
		(b) Service Desk scripting and system for Knowledge Management; and
		(c) Known Errors.
		13.4.4 The Service Requirements for Knowledge Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
04-03-01-001-03	3	NOT USED
04-03-01-002-03	3	NOT USED
04-03-01-003-03	3	NOT USED
04-03-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Knowledge Management Policies, Processes and Procedures.
04-03-01-014-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Knowledge Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
04-03-01-015-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Knowledge Management Policies, Processes and Procedures.
04-03-01-016-01	3	The Hosting Supplier shall provide Knowledge Management for Hosting Services in accordance with the SIAM Supplier's Knowledge Management Policies, Processes and Procedures.
	2	**Service Knowledge Management System**
04-03-02-002-01	3	The Hosting Supplier shall use the SKMS provided by the SIAM Supplier in line with the SIAM Supplier's Knowledge Management Policies and Procedures.

Requirement No.	Level	Requirement
04-03-02-004-01	3	The Hosting Supplier shall support the SIAM Supplier in the production, maintenance and assurance of up-to-date information for inclusion in the FITS SKMS, to include but not limited to : (i) Methods to resolve Incidents; (ii) Known Errors; (iii) Service Desk scripts; (iv) Self help articles; and (v) Frequently asked questions (FAQs).
	2	**Monitor and Report**
04-03-03-003-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to carry out conformance reviews and audits to ensure the integrity and accuracy of data in the SKMS.
04-03-03-005-01	3	When Hosting Supplier related data is found in the SKMS that is inaccurate, incomplete or lacks integrity, the Hosting Supplier shall support the SIAM Supplier in correcting or removing such data.
	2	**Knowledge Management communication**
04-03-04-002-01	3	The Hosting Supplier shall inform the SIAM Supplier of any new Changes to the Data within the Service Knowledge Management System (SKMS) in accordance with the Knowledge Management Policies and Procedures
	2	**Skills, Knowledge and Education**

Requirement No.	Level	Requirement
04-03-05-002-01	3	Where required, the Hosting Supplier shall attend the training sessions on utilisation of the SKMS organised by the SIAM Supplier.

Requirement No.	Level	Requirement
		13.5 Release and Deployment Management
		13.5.1 The Hosting Supplier shall provide Release and Deployment Management to support the following steps in the Release and Deployment Management lifecycle:
		(a) Review and update the Release Policy;
		(b) Accept Service Design Packages;
		(c) Build, test and deployment preparations;
		(d) Build and test;
		(e) Coordinate and manage Operational Acceptance Testing, Service Acceptance Testing and Pilot Testing;
		(f) Plan and prepare for deployment;
		(g) Transfer, deploy and retire and decommission;
		(h) Provide early life support;
		(i) Verify service deployment; and
		(j) Review and close deployment.
		13.5.2 The purpose for the Release and Deployment Management process is to assemble and position all elements of service into all controlled Authority ICT Environments and establish effective use of new or changed FITS Services, covering the full scope of Service Assets and Configuration Items.

Requirement No.	Level	Requirement
		13.5.3 The benefit of an effective and efficient Release and Deployment Management process is that it adds a consistent and effective means to deliver change in to all ICT controlled environments, minimising risk and cost. It also provides assurance to the Authority that new or changed FITS Services deployed on to the estate derive their full business benefit by establishing an auditable process for tracing requirements from development through to delivery.
		13.5.4 The Service Requirements for Release and Deployment Management are listed below:
	2	**General Requirements**
04-04-01-001-03	3	The Hosting Supplier shall provide a Release and Deployment Management function which will include planning, scheduling and controlling the build, Test and Deployment of Releases, and for delivering new functionality while protecting the integrity of existing Services.
04-04-01-002-03	3	NOT USED
04-04-01-003-03	3	NOT USED
04-04-01-004-03	3	NOT USED
04-04-01-005-03	3	The Hosting Supplier shall utilise the SIAM Supplier's Release and Deployment Management System.
04-04-01-006-03	3	NOT USED
04-04-01-007-03	3	NOT USED
04-04-01-008-03	3	NOT USED

Requirement No.	Level	Requirement
04-04-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Release and Deployment Management Policies, Processes and Procedures.
04-04-01-015-01	3	The Hosting Supplier shall provide to the SIAM Supplier their respective Release Plan(s) over a two month rolling period. Release Plan(s) shall provide a comprehensive forward planning view of Releases over an agreed period over a two month rolling period in accordance with the SIAM Supplier's Release and Deployment Management Policies and Procedures.
04-04-01-016-01	3	The Hosting Supplier shall support the SIAM Supplier in maintaining and updating the FITS Release Schedule and associated Release Plan(s) as per the SIAM Supplier's Release and Deployment Policies and Procedures.
04-04-01-020-01	3	The Hosting Supplier shall provide Release Documentation to the SIAM Supplier, including but not limited to: (i) Release Plans; (ii) Release Packages; and (iii) Implementation activities.
04-04-01-022-01	3	The Hosting Supplier shall produce and submit to the SIAM Supplier impact analysis and potential mitigating actions in support of the Release planning process.
04-04-01-025-01	3	The Hosting Supplier shall ensure that all Service Assets and Configuration Items included in a Release Package are updated in the CMS and in all relevant documentation as part of the execution of the Release in accordance with the SIAM Supplier's Release and Deployment Policies, Processes and Procedures.

Requirement No.	Level	Requirement
04-04-01-026-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Release and Deployment Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
04-04-01-027-01	3	The Hosting Supplier shall support the SIAM Supplier in identifying, Impact assessing and co-ordinating multiple Change Requests into a single planned Release to ensure successful implementation in accordance with the SIAM Supplier's Release and Deployment Management Policies, Processes and Procedures.
04-04-01-028-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to plan and implement Release activity to ensure that any business disruption is minimised.
04-04-01-029-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Release and Deployment Management Policies, Processes and Procedures.
04-04-01-030-01	3	The Hosting Supplier shall provide Release and Deployment Management for Hosting Service in accordance with the SIAM Supplier's Release and Deployment Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
		13.6 Service Asset and Configuration Management
		13.6.1 The purpose of Service Asset and Configuration Management (SACM) is to identify and control Service Assets and Configuration Items (CIs) by recording and reporting the status of Service Assets and CIs and by governing the performance of periodic audits to verify the accuracy and completeness of data held within appropriate repositories.
		13.6.2 Optimising the performance of Service Assets and configurations improves the overall service performance and optimises the costs and minimises risks caused by poorly managed Assets, e.g. service outages, incorrect licence fees and failed audits.
		13.6.3 Effective SACM can significantly improve the overall service performance by enabling the Hosting Supplier to:
		(a) Reduce the instances of quality and compliance issues;
		(b) Manage the compliance to Policies, standards, legal and regulatory obligations;
		(c) Manage service quality and costs;
		(d) Gain a better understanding of risk level during and after Change;
		(e) Optimise the performance of Service Assets and CIs thus delivering improved levels of service;
		(f) Minimises the disruption and costs associated with poorly managed Assets;

Requirement No.	Level	Requirement
		(g) Provides accurate information on all FITS Services and environments deployed and support Change Management; and
		(h) Scope Assets including any resource or capability. The Assets of a Supplier include anything that could contribute to the delivery of Service. Assets include but are not limited to:
		(i) Management;
		(ii) Organisation;
		(iii) Process;
		(iv) Knowledge;
		(v) People;
		(vi) Information;
		(vii) Applications ;
		(viii) Infrastructure ; or
		(ix) Financial capital.
		13.6.4 The Service Requirements for Service Asset and Configuration Management are listed below:
	2	**General Requirements**
04-05-01-001-03	3	NOT USED
04-05-01-002-03	3	NOT USED

Requirement No.	Level	Requirement
04-05-01-007-01	3	The Hosting Supplier shall perform Service Asset and Configuration Management activities in accordance with the SIAM Supplier's Service Asset and Configuration Management Policies, Processes and Procedures.
04-05-01-014-01	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Configuration Management Database (CMDB); or (ii) Implement a CMDB that supports the SIAM Supplier's Service Asset and Configuration Management Processes, Policies and Procedures and interfaces with the SIAM Supplier's CMDB
04-05-01-016-01	3	The Hosting Supplier shall identify and record the relationships between Configuration Items within their Service Portfolio and shall report the relationships to the SIAM Supplier in accordance with the SACM Policies, Processes and Procedures.
04-05-01-018-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Asset and Configuration Management Policies, Processes and Procedures.
04-05-01-023-01	3	The Hosting Supplier shall support the identification of CIs and Service Assets as required by the SIAM Supplier and in accordance with the SIAM Supplier's Service Asset and Configuration Management Policies, Processes and Procedures.
04-05-01-028-01	3	The Hosting Supplier shall provide and maintain a list of Hosting Supplier Personnel who require access to the CMDB.
04-05-01-031-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's SACM Policies, Processes and Procedures and implement any required corrective action that has been Approved.
04-05-01-032-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's SACM Policies, Processes and Procedures.

Requirement No.	Level	Requirement
04-05-01-033-01	3	The Hosting Supplier shall ensure Configuration Items for existing and new Hosting Services are correctly recorded in the SIAM Supplier's CMDB and that this CMDB is kept current and up to date in accordance with the SACM Policies, Processes and Procedures.
	2	**Audit, Monitoring and Reporting**
04-05-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier in providing Quality Assurance, data reconciliation and audit activities against CI's data held within the FITS CMDB and data held in the Hosting Supplier's CMDB to ensure compliance with the SIAM Supplier's Service Asset and Configuration Management Policies, Processes and Procedures
04-05-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier to identify and implement remedial actions where it has been identified that the CMDB has breached Thresholds relating to accuracy or currency set out in schedule 2.2 (Service Performance Management).
	2	**Updates to Configuration Management**
04-05-03-002-01	3	The Hosting Supplier shall support the SIAM Supplier to ensure updates to the CMS are performed in accordance with the SIAM Supplier's Service Asset and Configuration Management Policies and Procedures and within the Service Levels set out in schedule 2.2 (Service Performance Management).
04-05-03-004-01	3	The Hosting Supplier shall support the SIAM Supplier in ensuring that updates to the CMS are automatically synchronised unless otherwise agreed with the Authority.
04-05-03-007-01	3	The Hosting Supplier shall either interface with or make use of the DML provided by the SIAM Supplier.
04-05-03-009-01	3	The Hosting Supplier shall ensure that only Software contained in the DML is deployed to the Hosting Supplier ICT Environment.
04-05-03-012-01	3	The Hosting Supplier shall support the SIAM Supplier in the implementation of the Authority's Asset Management Policy.

Requirement No.	Level	Requirement
	2	**Asset Management**
04-05-04-001-03	3	The Hosting Supplier shall catalogue and maintain documentation for Assets used in the provision of the Hosting Services in accordance with the SACM Policies, Processes and Procedures. The documentation shall include, but not be limited to: (i) Warranty documentation (ii) Contract details
04-05-04-003-01	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Asset Management System; or (ii) Implement an Asset Management System that supports the Service Asset and Configuration Management Process and Service Asset and interfaces with the SIAM Supplier's Asset Management System.
04-05-04-004-01	3	The Hosting Supplier shall maintain accurate records of Assets used to deliver the Hosting Services. This includes both physical Assets and Software Assets and is irrespective of the ownership of each Asset. Where Suppliers use shared Assets then a reference should be made in the attributes to that Asset.
04-05-04-006-01	3	The Hosting Supplier shall ensure that they record all agreed attributes of an Asset so that it can be uniquely defined in accordance with the SIAM Supplier's SACM Policies, Processes and Procedures.
	2	**Disposal of Assets**
04-05-05-001-03	3	The Hosting Supplier shall develop, manage and maintain the process for secure disposal of Removable Media used in the delivery of the Hosting Services in accordance with the Authority's Asset Disposal Policy, and have the process Approved by the Authority within three (3) months of the Effective Date.

Requirement No.	Level	Requirement
04-05-05-002-01	3	The Hosting Supplier shall support the SIAM Supplier to ensure that Software is efficiently, effectively and when possible automatically removed (in accordance with the Authority's Asset Disposal Policies) or redeployed across the Hosting Supplier ICT Environments.
04-05-05-002-03	3	The Hosting Supplier shall remove and dispose of Assets identified as redundant and in compliance with the Authority's Asset Disposal Policies.
		13.7 Service Validation and Testing
		13.7.1 The Authority places a strong emphasis on the quality and value of Testing performed by Suppliers and ensuring their testing activities integrate into the Testing lifecycle. The Authority has defined an overarching Test Strategy covering the whole lifecycle, with which all Suppliers must comply. The Authority Test Strategy sets out a number of key principles to ensure that Testing representatives are engaged early in the lifecycle, have sufficient independence and operate in a repeatable and measurable manner to well defined products, processes and controls.
		13.7.2 All FITS Suppliers are required to create a Supplier Test Policy setting out their approach to testing for the scope of FITS Services they provide, aligned to the Authority Test Strategy.
		13.7.3 The Authority may assure the Hosting Supplier's testing processes, throughout the testing lifecycle.
		13.7.4 The Service Requirements for Service Validation and Testing are listed below:
	2	**Testing Policies and Procedures**
04-06-01-001-03 (Common)	3	All testing conducted by the Hosting Supplier shall comply with the Authority Test Strategy and the Testing Policies, Processes and Procedures.

Requirement No.	Level	Requirement
04-06-01-002-03 (Common)	3	The Hosting Supplier shall identify an appropriately qualified Account Test Manager within ten (10) Working Days of the Effective Date. The Account Test Manager shall be fully accountable for all Service Validation & Testing performed and/or supported by the Hosting Supplier during the Term.
04-06-01-003-03 (Common)	3	The Hosting Supplier shall ensure continuity in the identified Account Test Manager throughout the Term and the Account Test Manager shall be Key Personnel for the purposes of the Agreement.
04-06-01-004-03 (Common)	3	Not used
04-06-01-005-03 (Common)	3	All testing conducted and/or supported by the Hosting Supplier shall be carried out in accordance with the Approved Supplier Test Policy, unless otherwise agreed with the Authority. The Authority Test Strategy and the Testing Processes, Policies and Procedures shall take precedence in the event of conflicts with the Approved Supplier Test Policy.
04-06-01-006-03 (Common)	3	The Hosting Supplier shall support the Authority, Suppliers or Other Authority Providers in the creation of each Programme Test Strategy/Project Test Strategy and/or Project Test Plan/Release Test Plan as required, setting out the testing activities for the Future Service or change to an existing Service as applicable.
04-06-01-008-03 (Common)	3	The Hosting Supplier shall, when required by the Authority, produce a Programme/Project Test Strategy and/or Project/Release Test Plan and submit to the Authority to decide Approval.
04-06-01-009-03 (Common)	3	The Hosting Supplier shall appoint a suitably qualified Test Manager where the Hosting Supplier has responsibilities for conducting or supporting testing in relation to a project or change. The Hosting Supplier Test Manager shall be responsible for all testing performed or supported by the Hosting Supplier who shall be the Single Point of Contact for the Authority for all such Hosting Supplier testing activities.
04-06-01-010-03 (Common)	3	The Hosting Supplier shall not pass a Test Item out of a Test Phase until the associated Test Exit Criteria have been met, unless otherwise agreed with the Authority. Where the Authority provides agreement for the Hosting Supplier to continue, the Hosting Supplier shall create a remediation plan within five (5) Working Days and submit to the Authority to decide Approval.

Requirement No.	Level	Requirement
04-06-01-011-03 (Common)	3	The Hosting Supplier shall support Test Assurance activities conducted by or on behalf of the Authority. Such assurance activities do not diminish the Hosting Supplier's obligations to achieve the applicable Acceptance Criteria and Service Levels.
	2	**Standard Testing Toolset**
04-06-02-001-03 (Common)	3	The Hosting Supplier shall use the Standard Testing Toolset for the scope of testing for which it is identified as responsible, unless otherwise agreed with the Authority.
04-06-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the evaluation of the Standard Testing Toolset.
04-06-02-002-03	3	The Hosting Supplier shall provide the capability for repositories associated with the tools comprising the Standard Testing Toolset as well as the tools themselves to be accessible from each provisioned test environment requiring it.
04-06-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier in the provision, maintenance and support of the Standard Testing Toolset
	2	**Test Environment Provisioning & Management**
04-06-03-001-03 (Common)	3	Not used
04-06-03-002-03 (Common)	3	Before a test environment can be handed over to the requesting party, the Hosting Supplier shall verify that the test environment complies with the associated Test Environment Specification. The results and outcome shall be recorded in the CMDB in a manner that associates them directly with the test environment.
04-06-03-018-01	3	The Hosting Supplier shall ensure that Test Environments are treated as Service Assets that are managed in accordance with the SACM Policies, Processes and Procedures.
04-06-03-019-01	3	Not used

Requirement No.	Level	Requirement
04-06-03-021-01	3	The Hosting Supplier shall make available to the requesting Supplier, the Test Environments provisioned via the SIAM Supplier as set out in the Project Test Strategy or Release Test Plan.
04-06-03-022-01	3	The Hosting Supplier shall ensure that the Test Environments support maintenance and testing of Repairs made during and following the PRISM period.
	2	**Unit/Component Testing**
04-06-04-001-03 (Common)	3	The Hosting Supplier shall be fully accountable for the planning, design, implementation, execution and reporting for Unit/Component Testing for all new and/or modified components it is providing in relation to a project or change, as specified in the associated Test Strategy developed by or Approved by the Authority.
	2	**Component Integration Testing**
04-06-05-001-03 (Common)	3	The Hosting Supplier shall be fully accountable for the planning, design, implementation, execution and reporting for Component Integration Testing for all new and/or modified components it is providing in relation to a project or change, as specified in the associated Test Strategy developed by or Approved by the Authority.
04-06-05-002-03 (Common)	3	The Hosting Supplier shall ensure that where there are interfaces with other systems and/or external interfaces that early System Integration Testing is included within the Component Integration Testing (CIT) Test Plan, to de-risk the System Integration Testing test phase.
04-06-05-003-03 (Common)	3	The Hosting Supplier shall support Component Integration Testing (CIT) planning, design, implementation, execution and reporting conducted by the Suppliers and Other Authority Providers where required by the associated Test Strategy developed by or Approved by the Authority.
	2	**System Testing**
04-06-06-001-03 (Common)	3	The Hosting Supplier shall be accountable for the planning, design, implementation, execution and reporting for System Testing for all new and/or modified components it is providing in relation to a project or Change, as specified in the associated Test Strategy developed by or Approved by the Authority.

Requirement No.	Level	Requirement
04-06-06-002-03 (Common)	3	The Hosting Supplier shall support System Testing planning, design, implementation, execution and reporting conducted by other Suppliers and Other Authority Providers as identified in the associated Test Strategy developed by or Approved by the Authority.
	2	**Systems Integration Testing**
04-06-07-001-03 (Common)	3	The Hosting Supplier shall support the Authority in the planning, design, implementation, execution and reporting of System Integration Testing.
	2	**Operational Acceptance Testing**
04-06-08-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the planning, design, implementation, execution and reporting of Operational Acceptance Testing.
	2	**User Acceptance Testing**
04-06-09-001-03 (Common)	3	The Hosting Supplier shall support the Authority in the planning, design, implementation, execution and reporting of User Acceptance Testing.
	2	**Service Acceptance Testing**
04-06-10-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the planning, design, implementation, execution and reporting of Service Acceptance Testing.
	2	**Pilot Testing**
04-06-11-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the planning, design, implementation, execution and reporting of Pilot Testing.
	2	**Break/Fix Testing**

Requirement No.	Level	Requirement
04-06-12-001-03 (Common)	3	The Hosting Supplier shall be fully accountable for the planning, design, implementation, execution and reporting of Break/Fix Testing of the components for which it is responsible.
04-06-12-002-03 (Common)	3	The Hosting Supplier shall support the Suppliers and Other Authority Providers in the planning, design, implementation, execution and reporting of Break/Fix Testing.
	2	**Maintenance Release Testing**
04-06-13-001-03 (Common)	3	The Hosting Supplier shall be fully accountable for the planning, design, implementation, execution and reporting of Maintenance Release Testing of the components for which it is responsible.
04-06-13-002-03 (Common)	3	The Hosting Supplier shall support the Suppliers and Other Authority Providers in the planning, design, implementation, execution and reporting of Maintenance Release Testing.
	2	**Transfer of Test Assets for Live Service**
04-06-14-001-03 (Common)	3	The Hosting Supplier shall ensure that all Test Assets it has created or modified are incorporated into the Configuration Management Database in accordance with the SACM Processes, Policies and Procedures.

Requirement No.	Level	Requirement
		14. SERVICE OPERATION
		14.1 Introduction
		The purpose of Service Operation is the coordination and delivery of the activities, processes and functions required to deliver and manage FITS Services to agreed quality and Service Level Targets to the Authority. Service Operation covers the responsibilities for the ongoing management of the technology used to deliver and support FITS Services.
		14.2 Access Management
		14.2.1 Access Management is the process of granting authorised Users the right to use a FITS Service and helps to protect the confidentiality, integrity and availability of Assets and information.
		14.2.2 A controlled and managed Access Management process delivers benefit to the Authority by:
		(a) Ensuring that the organization is able to maintain the confidentiality of its information more effectively;
		(b) Employees having the right level of access to execute their jobs effectively;
		(c) The ability to audit use of services and to trace the abuse of services; and
		(d) The ability to easily revoke access rights when needed.
		14.2.3 The Service Requirements for Access Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
05-01-01-001-03	3	NOT USED
05-01-01-002-03	3	NOT USED
05-01-01-003-03	3	NOT USED
05-01-01-004-03	3	NOT USED
05-01-01-005-01	3	The Hosting Supplier shall comply with the Authority's Access Management Policy, and the SIAM Supplier's Access Management Processes and Procedures, unless otherwise agreed with the Authority.
05-01-01-005-03 (Common)	3	The Hosting Supplier shall comply with the Authority Access Management Policy and the SIAM Supplier's Supplier Personnel Access Management Processes and Procedures, when the Hosting Supplier's Personnel requires access to Authority Sites, Other Supplier's Sites or Other Supplier's ICT Environment.
05-01-01-006-03	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Supplier Personnel Access Management Processes and Procedures and implement any required corrective action that has been Approved.
05-01-01-008-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the Authority's Access Management Policy and the SIAM Supplier's Access Management Processes and Procedures and implement any required corrective action, unless otherwise agreed with the Authority.
05-01-01-009-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the Authority's Access Management Policies and the SIAM Supplier's Operational Processes and Procedures and implement any required corrective action that has been Approved.
05-01-01-013-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Operational Processes and Procedures.

Requirement No.	Level	Requirement
	2	**User Administration**
05-01-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier to define, implement and maintain FITS Services in accordance with the SIAM Supplier's User Administration Policy, Processes and Procedures.
05-01-02-003-01	3	NOT USED
05-01-02-010-01	3	The Hosting Supplier shall comply with the SIAM Supplier's User Administration Policy, Processes and Procedures, unless otherwise agreed with the Authority.
	2	**Third Party Hosted Application Access**
05-01-03-004-01	3	Where the Hosting Supplier hosts Other FITS Suppliers or Other Authority Provider's Business Applications or Services in the Hosting Supplier's ICT Environment. The Hosting Supplier shall provide secure access to the Other Suppliers or Other Authority Provider, to enable them to support their Business Application or Services.
05-01-03-005-01	3	The Hosting Supplier shall ensure that access to the Other Supplier's or Other Authority Provider's Business Application or Services is provided in accordance with Authority's Access Management Policy, the SIAM Supplier's User Administration Policy and the SIAM Supplier's Access Management Procedures.
	2	**Access Management Dependencies**
	3	Not applicable

Requirement No.	Level	Requirement
		14.3 Event Management
		14.3.1 The Event Management process shall detect Events, analyse and then determine the appropriate control activity or action to prevent an Incident and/or service interruption.
		14.3.2 Events need to be identified and set up such that their occurrence enables the communication of operational information.
		14.3.3 The benefit of effective Event Management to the Authority is that it:
		(a) Provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action before any actual service outage occurs;
		(b) Can signal, when integrated into other Service Management processes, status changes or exceptions that allow the appropriate person or team to respond promptly, thus improving the performance of the process; and
		(c) Provides a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work.
		14.3.4 The Service Requirements for Event Management are listed below:
	2	**General Requirements**
05-02-01-001-03	3	NOT USED

Requirement No.	Level	Requirement
05-02-01-002-03	3	The Hosting Supplier shall identify and implement improvements to Event Management for Hosting Services.
05-02-01-003-03	3	NOT USED
05-02-01-004-03	3	NOT USED
05-02-01-005-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Event Management System; or (ii) Implement an Event Management System that supports the SIAM Supplier's Event Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Event Management System.
05-02-01-008-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Event Management Policies, Processes and Procedures.
05-02-01-014-01	3	The Hosting Supplier shall provide Event monitoring information to the SIAM Supplier in accordance with the Event Management Policies, Processes and Procedures.
05-02-01-016-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Event Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
05-02-01-017-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the SIAM Supplier's Event Management Policies, Processes and Procedures.
05-02-01-018-01	3	The Hosting Supplier shall provide Event Management for Hosting Services in accordance with the SIAM Supplier's Event Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
	2	**Support Alert Management**
05-02-02-001-03	3	NOT USED
05-02-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the investigation and resolution of Events that have exceeded a pre defined Threshold.
05-02-02-002-03	3	NOT USED
05-02-02-003-01	3	The Hosting Supplier shall record and track Alerts by volume, type, service components and services and produce trend analysis as required by the SIAM Supplier.
05-02-02-003-03	3	NOT USED
05-02-02-004-03	3	NOT USED
05-02-02-005-01	3	The Hosting Supplier shall provide defined event thresholds to the SIAM Supplier for inclusion in the SIAM Supplier's Event Management Policies, Processes and Procedures.
	2	**Event Filtering**
05-02-03-001-01	3	The Hosting Supplier shall ensure that the SIAM Supplier is informed of any corrective action taken to address an Event and that the relevant records are updated in accordance with the SIAM Supplier's Event Management Policies, Processes and Procedures
	2	**Event Management communication**
	3	Not applicable

Requirement No.	Level	Requirement
		14.4 Incident Management
		14.4.1 The Authority requires Incident Management to be the process that handles all Failures, Faults or questions reported by End Users via the Service Desk or which are automatically detected and reported by Event Management. Incident Management should include the use of Incident Models that include the following steps within the Incident Management lifecycle:
		(a) Log and categorisation of the Incident;
		(b) Diagnosis and the steps required to handle the Incident;
		(c) Assign responsibilities for the performance and execution of first-level, second-level and third-level support, analysis, diagnosis and resolution of the incident;
		(d) Set expectations on timescales and Thresholds for the completion of identified actions;
		(e) Manage the escalation activities based on pre-defined hierarchy and communication plan;
		(f) Identify measures, when appropriate, to minimise future disruptions; and
		(g) Manage the end-to-end Incident lifecycle.
		14.4.2 The purpose of Incident Management is to restore the FITS Services as quickly as possible and minimising adverse impact and disruption on normal business operations.
		14.4.3 Effective Incident Management allows the business to continue to realise the benefits of enabling ICT technologies and services by:

Requirement No.	Level	Requirement
		(a) Minimising downtime of the FITS Services, and where applicable the End to End Services, to the business;
		(b) Ensuring FITS Services are aligned with day-to-day business priorities;
		(c) Identifying potential service improvements; and
		(d) Identifying additional service or training requirements.
		14.4.4 The Service Requirements for Incident Management are listed below:
	2	**General Requirements**
05-03-01-001-03	3	NOT USED
05-03-01-006-01	3	The Hosting Supplier shall support the SIAM Supplier in developing, documenting, implementing and maintaining Incident Management Processes in accordance with the SIAM Supplier's Incident Management Policies and Procedures.
05-03-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Incident Management Policies, Processes and Procedures.
05-03-01-014-01	3	The Hosting Supplier shall proactively support the SIAM Supplier to deliver the required Service Levels, for Incident Management as defined in schedule 2.2 (Service Performance Management).
05-03-01-015-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Incident Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
05-03-01-018-01	3	The Hosting Supplier shall utilise the SIAM Supplier's Incident Management System.

Requirement No.	Level	Requirement
05-03-01-021-01	3	The Hosting Supplier shall ensure that the Incident Management process within their own organisation provides an audit trail that complies with the SIAM Supplier's Incident Management Policies, Processes and Procedures relating to the management and resolution of Incidents.
05-03-01-023-01	3	The Hosting Supplier shall adopt and implement the Severity and Priority Definitions as set out in schedule 2.2 (Service Performance Management).
05-03-01-025-01	3	The Hosting Supplier shall monitor and manage allocated Incidents for which they are responsible in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures and with the Service Levels set out in schedule 2.2 (Service Performance Management).
05-03-01-030-01	3	The Hosting Supplier shall update the Incident record with all relevant information relating to the Incident in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures.
05-03-01-033-01	3	The Hosting Supplier shall adhere to the Severity and Priority Definitions in accordance with the Priority Levels as specified by the Authority in schedule 2.2 (Service Performance Management).
05-03-01-035-01	3	The Hosting Supplier shall support the SIAM Supplier in the continual improvement of the Incident Management Processes via the identification and implementation of means by which the volume of Incidents are reduced over the term of the Agreement.
05-03-01-037-01	3	The Hosting Supplier shall provide Incident Management for Hosting Services in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures.
	2	**Provide Incident Management Support**
05-03-02-001-03	3	NOT USED
05-03-02-003-01	3	The Hosting Supplier shall provide appropriately skilled resources to fulfil their obligations as set out in the SIAM Supplier's Incident Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
05-03-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier to restore normal FITS Services or provide an Approved workaround during the resolution of Incidents.
05-03-02-010-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to manage the implementation of any temporary and permanent fixes to Systems Software in accordance with the SIAM Supplier's Incident and Problem Management Policies, Processes and Procedures.
	2	**Monitoring and Reporting of Incident Management**
05-03-03-001-01	3	The Hosting Supplier shall provide progress notifications to the SIAM Supplier on all current Incidents including progress notifications where the frequency of such notifications is in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures and the Service Levels as set out in schedule 2.2 (Service Performance Management).
05-03-03-001-03	3	NOT USED
05-03-03-005-01	3	The Hosting Supplier shall make changes to the assigned Priority Level of an Incident when directed to do so by the SIAM Supplier.
	2	**Incident Management Education**
	3	Not applicable
	2	**Incident Management Access**
	3	Not applicable
	2	**Incident Communications**
05-03-06-001-03	3	The Hosting Supplier shall provide the SIAM Supplier with contact Information for Resolver Groups within thirty (30) Working Days of the TSA Effective Date.

Requirement No.	Level	Requirement
05-03-06-002-01	3	The Hosting Supplier shall proactively notify the SIAM Supplier of any Incident to a Hosting Service that is known to be in breach or highly likely to breach its Service Level and/or Service Level Target as defined in schedule 2.2 (Service Performance Management) via the Service Desk.
05-03-06-002-03	3	NOT USED
05-03-06-003-01	3	The Hosting Supplier shall notify the SIAM Supplier in advance of any amendments to contact information for the Resolver Groups.
	2	**Support Incident Management**
05-03-07-001-01	3	The Hosting Supplier shall accept and acknowledge that the SIAM Supplier shall be the single point of contact with the Authority for the formal progression of all Incidents unless otherwise set out in the SIAM Supplier's Incident Management Policies, Processes and Procedures.
05-03-07-003-01	3	The Hosting Supplier shall acknowledge all Incidents correctly assigned to them and return Incidents to the SIAM Supplier that have been wrongly assigned in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures.
05-03-07-004-01	3	The Hosting Supplier following receipt of an Incident shall, where necessary, schedule and perform resolution activities with the End User in accordance with the SIAM Supplier's Incident Management Policies, Processes and Procedures.
05-03-07-006-01	3	The Hosting Supplier shall co-operate, provide information and support to the Other Suppliers as identified in the Dependencies Register in order to aid the resolution of Incidents.
05-03-07-009-01	3	The Hosting Supplier shall provide updates to the SKMS as a result of an Incident, in accordance with the SIAM Supplier's Knowledge Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
		14.5 Problem Management
		14.5.1 Problem Management deals with the underlying causes of incidents. The functionality of Problem Records should be similar to those needed for Incident Records and also allow for multiple incidents matching against Problem Records. This service shall include the following steps in the Problem Management lifecycle:
		(a) Detection;
		(b) Capture and categorisation;
		(c) Investigation and diagnosis; and
		(d) Resolution.
		14.5.2 The principle objective of Problem Management is to prevent Problems from occurring by eliminating recurring Incidents and to minimise the impact of Incidents that cannot be prevented.
		14.5.3 Effective Problem Management reduces the impacts to the business of reduced service quality in FITS Services, allowing the business to continue to realise the benefits of enabling ICT technologies and services by:
		(a) Reducing the number of Incidents raised across the estate;
		(b) Employing Root Cause Analysis to determine cause of Problems and to further eliminate potential issues;

Requirement No.	Level	Requirement
		(c) Implementing a permanent fix for all identified problem causes; and
		(d) Logging and maintaining Known Errors and workarounds to prevent FITS Service outage.
		14.5.4 The Service Requirements for Problem Management are listed below:
	2	**General Requirements**
05-04-01-001-03	3	NOT USED
05-04-01-002-03	3	NOT USED
05-04-01-003-03	3	NOT USED
05-04-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Problem Management Policies, Processes and Procedures.
05-04-01-019-01	3	The Hosting Supplier shall utilise the SIAM Supplier's Problem Management system and tooling in support of Problem Management process and procedures in the delivery on the Hosting Services, via the SIAM Supplier's standard interface.
05-04-01-021-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Problem Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
05-04-01-022-01	3	The Hosting Supplier shall provide Problem Management for the Hosting Service in accordance with the SIAM Supplier's Problem Management Policies, Processes and Procedures.
05-04-01-023-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the Problem Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
	2	**Monitor and Report**
05-04-02-002-01	3	The Hosting Supplier shall monitor and progress, in line with the Service Levels set out in schedule 2.2 (Service Performance Management) for the Problems for which they are responsible in accordance with the SIAM Supplier's Problem Management Policies, Processes and Procedures.
05-04-02-007-01	3	The Hosting Supplier shall develop, maintain and provide to the SIAM Supplier, for inclusion in the SKMS, Information on Workarounds, Known Errors and Problems related to Hosting Services.
	2	**Managing the Problem Management Lifecycle**
05-04-03-002-01	3	The Hosting Supplier shall support the SIAM Supplier in Problem analysis as requested by the SIAM Supplier including, but not limited to, the provision of information relating to Problem trends, volumes and Problem solutions.
05-04-03-011-01	3	The Hosting Supplier shall attend Problem reviews as requested by the SIAM Supplier and in accordance with the SIAM Supplier's Problem Management Policies, Processes and Procedures
	2	**Support for Problem Management**
05-04-04-001-01	3	The Hosting Supplier shall provide status updates on Problem resolution to the SIAM Supplier in accordance with the SIAM Supplier's Problem Management Policies, Processes and Procedures.
05-04-04-001-03	3	NOT USED
05-04-04-002-01	3	The Hosting Supplier shall resolve Problems that have been assigned to them by the SIAM Supplier in accordance with the SIAM Supplier's Problem Management Policies, Processes and Procedures.
05-04-04-002-03	3	NOT USED
05-04-04-003-03	3	NOT USED

Requirement No.	Level	Requirement
05-04-04-004-03	3	The Hosting Supplier shall request Third Party Providers to implement Authority Approved Root Cause Analysis recommendations.
		14.6 Request Fulfilment
		14.6.1 Request Fulfilment is the process for managing Service Requests. These standard and repeatable changes are initiated via an automated catalogue of FITS Services and follow the steps within the Request Fulfilment lifecycle.
		14.6.2 The benefit of a centralised, efficient and effective Request Fulfilment process is:
		(a) A fast and efficient service improves productivity by delivering services when they are required;
		(b) Improvement to the quality services used through the use of centralised procurement and fulfilment;
		(c) Improved process conformance and reduction in unnecessary bureaucracy and administration in submitting requests and delivering services; and
		(d) Greater control over the FITS Services on offer.
		14.6.3 The Service Requirements for Request Fulfilment are listed below:
	2	**General Requirements**
05-05-01-001-03	3	The Hosting Supplier shall provide Request Fulfilment for Hosting Services in accordance with the Request Fulfilment Policies, Processes and Procedures.
05-05-01-002-03	3	The Hosting Supplier shall utilise the SIAM Supplier Request Fulfilment System.

Requirement No.	Level	Requirement
05-05-01-003-03	3	NOT USED
05-05-01-008-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Request Fulfilment Policies, Processes and Procedures
05-05-01-018-01	3	The Hosting Supplier shall action each Service Request they receive from the SIAM Supplier in accordance with the SIAM Supplier's Request Fulfilment Policies, Processes and Procedures and in accordance with schedule 2.2 (Service Performance Management).
05-05-01-024-01	3	The Hosting Supplier shall notify the SIAM Supplier of any potential breach to the Service Levels as defined in schedule 2.2 (Service Performance Management) relating to Service Requests.
05-05-01-025-01	3	The Hosting Supplier shall support the SIAM Supplier in the identification and resolution of conflicts in the fulfilment of competing Service Requests.
05-05-01-027-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Request Fulfilment Policies, Processes and Procedures and implement any required corrective action that has been Approved.
05-05-01-028-01	3	The Hosting Supplier shall support the SIAM Supplier in the maintenance of the Request Fulfilment Policies, Processes and Procedures.
	2	**Monitoring and Reporting**
05-05-02-001-03	3	NOT USED
05-05-02-003-01	3	The Hosting Supplier shall support the SIAM Supplier in analysing and reporting on Request Fulfilment as requested by the SIAM Supplier and in accordance with the SIAM Supplier's Request Fulfilment Policies, Processes and Procedures
05-05-02-007-01	3	The Hosting Supplier shall provide status updates on Service Requests to the SIAM Supplier in accordance with SIAM Supplier's Request Fulfilment Policies, Processes and Procedures.

Requirement No.	Level	Requirement
		14.7 Service Desk
		14.7.1 The SIAM Service Desk function shall provide a single point of contact for all FITS Services provided to the Authority. It shall consist of appropriately skilled staff responsible for dealing with a variety of service Events and should be able to:
		(a) Leverage expert resource from the Other FITS Suppliers;
		(b) Handle all Incidents and Service Requests; and
		(c) Utilise specialist tools to manage all Events.
		14.7.2 The primary aim of the SIAM Service Desk shall be to restore normal service to the End Users as quickly as possible.
		14.7.3 The Service Requirements for supporting the SIAM Service Desk are listed below:
	2	**General requirements**
05-06-01-001-03	3	The Hosting Supplier shall provide Resolver Groups to support its Service Management obligations relating to the Hosting Services.
05-06-01-013-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Desk Policies, Processes and Procedures and provide the required Service Support for the Service or Service Components to fulfil the Service Levels defined in schedule 2.2 (Service Performance Management).
05-06-01-014-01	3	The Hosting Supplier shall provide English speaking resources to support SIAM Supplier's Service Desk in the provision of ITIL processes.

Requirement No.	Level	Requirement
05-06-01-016-01	3	The Hosting Supplier shall provide updates and information and interface with the Incident, Change and Service Request lifecycle as defined in the SIAM Supplier's Service Desk Policies, Processes and Procedures.
05-06-01-024-01	3	The Hosting Supplier shall support the SIAM Supplier in the provision of a Service Desk function in accordance with the SIAM Supplier's Service Desk Policies, Processes and Procedures.
05-06-01-025-01	3	The Hosting Supplier shall provide the SIAM Supplier with all appropriate information on Incidents, Problems, Known Errors, Approved workarounds, Hosting Supplier's Releases and their inter-relationships in support of FITS Services.
05-06-01-027-01	3	The Hosting Supplier shall support the SIAM Supplier in delivery of Service Desk services.
05-06-01-028-01	3	Not used
05-06-01-029-01	3	Not used
	2	**Skills, Knowledge and Education**
05-06-02-002-01	3	The Hosting Supplier shall ensure that personnel who interact with the Service Desk are appropriately trained and are capable of working to the SIAM Supplier's Incident Management, Problem Management, Service Request and Knowledge Management Policies, Processes and Procedures.
05-06-02-005-01	3	The Hosting Supplier shall ensure that personnel who interact with the Service Desk have access to the Service Knowledge Management System or shall support the SIAM Supplier to ensure that the personnel of the Hosting Supplier be granted access to the SIAM Supplier's SKMS.
	2	**Communication**
05-06-03-003-01	3	The Hosting Supplier shall ensure that all first contact communication with End Users is managed and coordinated via the SIAM Supplier's Service Desk.

Requirement No.	Level	Requirement
05-06-03-004-01	3	The Hosting Supplier shall ensure that all subsequent (after first contact) communication with End Users is recorded in the Incident Record and is made available to the SIAM Supplier's Service Desk in accordance with the Service Desk Policies, Processes and Procedures.
05-06-03-005-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to ensure the Hosting Supplier can provide information about Incidents and Problems that occur in the Live Environments at different Business Impact Levels.

Requirement No.	Level	Requirement
		14.8 Technical Management
		14.8.1 Technical Management is the process for managing the routine maintenance activities of the technical components of the Hosting Service, including:
		(a) LAN and WAN components;
		(b) Hardware; and
		(c) Software.
		14.8.2 The purpose of Technical Management is to perform the proactive and reactive maintenance activities required to keep the FITS Services, and where applicable the End to End Services, in a Fully Functional state to minimise adverse impact and disruption on normal business operations.
		14.8.3 Effective Technical Management allows the business to continue to realise the benefits of enabling ICT technologies and services by:
		(a) Minimising downtime of the FITS Services, and where applicable the End to End Services, to the business;
		(b) Ensuring FITS Services are aligned with day-to-day business priorities; and
		(c) Maintaining alignment between FITS Services and technology roadmaps.
		14.8.4 The Service Requirements for Technical Management are listed below:
	2	**LAN Management**

Requirement No.	Level	Requirement
05-07-01-001-03	3	The Hosting Supplier shall provide, maintain, manage and support LAN components of the Hosting Service in accordance with schedule 2.2 (Service Performance Management), schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan).
05-07-01-002-03 (Common)	3	The Hosting Supplier shall ensure that all Software used on Network Devices implemented in the ICT Environment for the delivery of Hosting Services is not more than five (5) years old and has at least three (3) years support available unless otherwise agreed by the Authority.
	2	**WAN Management**
05-07-02-001-03 (Common)	3	The Hosting Supplier shall ensure that all Software used on Network Devices implemented in the ICT Environment used for the delivery of Hosting Services is not more than five (5) years old and has at least three (3) years support available unless otherwise agreed by the Authority.
05-07-02-002-10	3	The Hosting Supplier shall manage and support the dark fibre or equivalent connectivity, provided by the Data Centre Supplier for cross site connectivity between the Data Centre Facilities.
	2	**End User Services Hardware Maintenance and Support**
	3	Not applicable
	2	**Technical Infrastructure Services Hardware Maintenance and Support**
05-07-04-001-01	3	The Hosting Supplier shall perform emergency maintenance to the Hosting Supplier ICT Environments in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
05-07-04-001-03	3	The Hosting Supplier shall maintain, manage and support all Devices and components used in the delivery of Hosting Services in accordance with schedule 2.2 (Service Performance Management), schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan), to ensure Availability of FITS Services.

Requirement No.	Level	Requirement
05-07-04-002-01	3	The Hosting Supplier shall schedule and implement installations of, upgrades to, and customisations of, the Hosting Services in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
05-07-04-002-03	3	NOT USED
05-07-04-003-01	3	The Hosting Supplier shall perform routine maintenance to the Hosting Service and associated Hosting Supplier ICT Environments in accordance with the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures.
05-07-04-003-03	3	NOT USED
05-07-04-004-03	3	NOT USED
05-07-04-005-03	3	The Hosting Supplier shall comply with warranty conditions applicable to the Devices used in the delivery of Hosting Services.
05-07-04-006-03	3	The Hosting Supplier shall assume responsibility for the warranty and maintenance requirements for any Authority Asset that is used in the delivery of the Hosting Service.
	2	**Client Software Maintenance and Support**
05-07-05-001-03 (Common)	3	The Hosting Supplier shall ensure that all Client Software provided by the Hosting Supplier in support of the Hosting Services is maintained in Fully Functional condition.

Requirement No.	Level	Requirement
05-07-05-002-03 (Common)	3	The Hosting Supplier shall ensure that all Client Software implemented in the ICT Environment for the delivery of Hosting Services is not more than five (5) years old and has at least three (3) years support available unless otherwise agreed by the Authority. Client Software covered by this provision includes, but is not limited to: (i) Operating System (ii) Collaboration Toolset (iii) Archiving Service (iv) Internet browsers and plug-ins (v) PDF reader (vi) Software used in the protection against computer virus, malicious code, malware and vulnerabilities. (vii) Device control
	2	**System Software Maintenance and Support**
05-07-06-001-03	3	The Hosting Supplier shall provide support for and maintenance of System Software deployed for the Hosting Services.
05-07-06-002-03	3	The Hosting Supplier shall provide, maintain, manage support and document System Software components of the Hosting Service in accordance with schedule 2.2 (Service Performance Management), schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan), to ensure Availability of FITS Services.
05-07-06-003-01	3	The Hosting Supplier shall ensure that all vendor recommended maintenance releases to System Software are tested and scheduled for release in accordance with the SIAM Supplier's Release and Deployment Management process.

Requirement No.	Level	Requirement
05-07-06-003-03	3	The Hosting Supplier shall ensure that all System Software, unless otherwise agreed by the Authority, is supported by the Software vendor. Where an open source software product is utilised as System Software then for the purposes of this Agreement, the Hosting Supplier shall be treated as the vendor.
05-07-06-004-03 (Common)	3	The Hosting Supplier shall ensure that all System Software implemented in the ICT Environment for the delivery of Hosting Services is not more than five (5) years old and has at least three (3) years support available unless otherwise agreed by the Authority. System Software covered by this provision includes, but is not limited to: (i) Operating System (ii) Virtualisation Software (iii) Presentation Software (iv) Middleware Software (v) Database Software (vi) Web Hosting Software (vii) ITSM Toolset (viii) Gateway Services System Software (ix) Collaboration Toolset System Software (x) Archiving Service System Software (xi) Software used in the protection against computer virus, malicious code, malware and vulnerabilities. (xii) Device control

Requirement No.	Level	Requirement
05-07-06-005-03	3	NOT USED
05-07-06-006-03	3	NOT USED
05-07-06-007-03	3	The Hosting Supplier shall ensure that all vendor recommended maintenance releases to System Software are tested and prepared for implementation within three (3) Months of Release by the vendor unless otherwise agreed.
05-07-06-008-03	3	The Hosting Supplier shall produce an Impact Analysis, a review of options and an implementation plan for the recommended option, to be submitted to the Authority to review and decide Approval, within three (3) Months of a new major release of a System Software product currently utilised by the Hosting Service becoming available.
	2	**Enhanced User Support**
	3	Not applicable
		14.9 Operational Management
		14.9.1 Operational Management is the overarching processes and activities required for the ongoing management of the technology used to deliver and support FITS Services.
		14.9.2 The Service Requirements for Operational Management are listed below:
	2	**General requirements**
	3	Not applicable

Requirement No.	Level	Requirement
		14.10 Application Management
		14.10.1 The Service Requirements for Application Management are listed below:
	2	**General Requirements**
	3	Not applicable
	2	**Application Maintenance and Support**
	3	Not applicable
	2	**Security and Hardening**
	3	Not applicable
	2	**Application Batch Management**
	3	Not applicable

Requirement No.	Level	Requirement
		15. CONTINUAL SERVICE IMPROVEMENT
		15.1 Introduction
		15.1.1 The purpose of Continual Service Improvement (CSI) is to create and maintain value in the design, introduction, operation and use of FITS Services. Through the process of Plan-Do-Check-Act; then Service Improvement Plans are created based on shortfalls or opportunities identified.
		15.2 Identify and Deliver Service Improvement
		15.2.1 This service shall include the following steps in the Continual Service Improvement lifecycle:
		(a) Reviewing management information and trends to ensure that the output of the enabling ITSM processes are achieving the desired results;
		(b) Periodically conducting maturity assessments against the process activities and roles associated with the process activities to demonstrate areas of improvement or, conversely, areas of concern;
		(c) Periodically conducting audits verifying process compliance;
		(d) Reviewing the FITS Services for improvements;
		(e) Making recommendations for Approval; and
		(f) Conducting periodic customer satisfaction surveys.

Requirement No.	Level	Requirement
		15.2.2 The primary purpose of CSI is to continually align and realign the FITS Services to the changing Authority needs by identifying and implementing improvements to FITS Services that support the Authority's core business. Improvement activities shall support the lifecycle approach through Service Strategy, Service Design, Service Transition and Service Operations.
		15.2.3 The benefit of 'Identify and Deliver Service Improvement' is that it:
		(a) Leads to a continual improvement in Service quality;
		(b) Ensures that FITS Services remain continuously aligned to business requirements;
		(c) Delivers improvements in cost effectiveness through identifying and implementing reduction in costs and or the capability to improve productivity; and
		(d) Identifies opportunities for improvement in all lifecycle stages and processes through monitoring and reporting.
		15.2.4 The Service Requirements for Identify and Deliver Service Improvement are listed below:
	2	**General requirements**
06-01-01-001-03	3	The Hosting Supplier shall provide Continual Service Improvement for Hosting Services
06-01-01-002-01	3	The Hosting Supplier shall ensure that Continual Service Improvement at all times effectively interfaces with all other processes across the Service Delivery Life Cycle.
06-01-01-002-03	3	NOT USED

Requirement No.	Level	Requirement
06-01-01-003-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Continual Service Improvement Policies, Processes and Procedures.
06-01-01-003-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Continual Service Improvement System; or (ii) Implement a Continual Service Improvement System that supports Continual Service Improvement and interfaces with the SIAM Supplier's Continual Service Improvement System.
	2	**Manage and Coordinate**
06-01-02-002-01	3	The Hosting Supplier shall support the SIAM Supplier in identifying and delivering Continual Service Improvement to FITS Services.
	2	**Continual Service Improvement Programme**
06-01-03-001-03	3	The Hosting Supplier shall attend the Continual Service Improvement Governance Board for each SRP
06-01-03-004-01	3	The Hosting Supplier shall support the SIAM Supplier in the production, maintenance and provision of Service Improvement Plans for those elements of the FITS Services for which they are responsible and have been identified as being the subject of improvements.
06-01-03-008-01	3	The Hosting Supplier shall engage and contribute in the establishment and delivery of the Continual Service Improvement Programme.
06-01-03-010-01	3	The Hosting Supplier shall ensure that they effectively discharge their obligations set out in the relevant Service Improvement Plan to ensure that such Service Improvement Plans are implemented effectively in accordance with the Continual Service Improvement Programme.

Requirement No.	Level	Requirement
	2	**Support for Service Improvement Programme**
06-01-04-002-01	3	The Hosting Supplier shall keep the SIAM Supplier informed of the progress against those Service Improvement Plans where the Hosting Supplier are responsible, in whole or part, for the delivery of those Service Improvement Plans
	2	**Service Maturity**
06-01-05-002-01	3	The Hosting Supplier shall support the SIAM Supplier in the establishment of a maturity assessment approach for the maturity of all Service Management processes and FITS Services to industry standard measures and criteria for measuring service maturity.
06-01-05-005-01	3	The Hosting Supplier shall support the SIAM Supplier to identify and implement opportunities for the continual improvement of the maturity of the Processes and FITS Services.

Requirement No.	Level	Requirement
		15.3 Service Measurement and Performance Management
		15.3.1 The Service Measurement and Performance Management process shall monitor the performance of the management of FITS Services and Service Management Framework. The Service Measurement and Performance Management process defines appropriate measures, collects and collates data and provides analytical reports that support the identification and delivery of service improvements. The Service Measurement and Performance Management process is set against organisational objectives and targets, as opposed to Service Level Management that is centred on contractual obligations and the monitoring and measurement against Service Level Targets and KPI.
		15.3.2 The benefit of an effective Service Measurement and Performance Management process is that it:
		(a) Aids and assists the decision making process for ICT Strategy attainment;
		(b) Provides information on the performance, availability, capacity and reliability of FITS Services;
		(c) Provides information on the performance of FITS Services;
		(d) Helps to identify the areas for service and process improvement;
		(e) Provides the means to assess the effectiveness of service and process improvements; and
		(f) Provides benchmark and baseline performance data that enable benchmarking activities.
		15.3.3 The Service Requirements for Service Measurement and Performance Management are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
06-02-01-001-03	3	NOT USED
06-02-01-002-03	3	NOT USED
06-02-01-003-03	3	NOT USED
06-02-01-004-03	3	The Hosting Supplier shall either: (i) Utilise the SIAM Supplier's Service Measurement and Performance Management System; or (ii) Implement a Service Measurement and Performance Management System that supports the Service Measurement and Performance Management Policies, Processes and Procedures and interfaces with the SIAM Supplier's Service Measurement and Performance Management System.
06-02-01-005-01	3	The Hosting Supplier shall support the SIAM Supplier and the Authority to develop a strategy for Service Measurement and Performance Management.
06-02-01-008-01	3	The Hosting Supplier shall support the SIAM Supplier to define and maintain the Policies, Processes and Procedures for Service Measurement and Performance Management.
06-02-01-009-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier's Service Measurement and Performance Management Policies, Processes and Procedures.
06-02-01-015-01	3	The Hosting Supplier shall support the SIAM Supplier in identifying any improvements to Service Measurement and Performance in accordance with the Continual Service Improvement Service.
06-02-01-017-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier's non compliance with the SIAM Supplier's Service Measurement and Performance Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.

Requirement No.	Level	Requirement
	2	**Performance Monitoring**
06-02-02-002-01	3	The Hosting Supplier shall support the Service Measurement and Performance Management process and ensure that there are effective interfaces with all FITS Services.
06-02-02-007-01	3	The Hosting Supplier shall support the SIAM Supplier in providing Service Measurement and Performance processes that use a reporting process that contains measurements that are 'SMART (Specific, Measureable, Attainable, Realistic and Time-bound)'.
06-02-02-010-01	3	The Hosting Supplier shall support the SIAM Supplier in providing a performance monitoring framework capable of providing different perspectives supporting, but is not limited to: (i) the use of a Balance Scorecard approach showing a mixture of quantitative and qualitative measures; (ii) the differing requirements of the Authority's User Profile; (iii) presents IT control performance information to industry Standards (e.g. COBIT); (iv) viewable data by the Authority's Business Unit and/or service consumed by Business Unit and/or Authority Site; and (v) sufficient granularity to identify the effects of poor performance and implemented service improvements.
06-02-02-016-01	3	The Hosting Supplier shall support the SIAM Supplier in the creation and maintenance of the Systems of Measurement Reference Document in conformance with the Service Transition requirements as specified in the Hosting Supplier's Tower Service Agreement.
06-02-02-017-01	3	The Hosting Supplier shall, for those Service Levels they are responsible for delivering against, implement and maintain the measurement criteria as defined in the Systems of Measurement Reference Document.

Requirement No.	Level	Requirement
06-02-02-019-01	3	The Hosting Supplier shall support the SIAM Supplier in providing performance information that: (i) Enables evaluation of performance of Hosting Services against stated Service Levels, Authority objectives and other agreed performance measures; and (ii) Enables comparison analysis of service performance against past, present and forecast of future predictions.
06-02-02-021-01	3	The Hosting Supplier shall support the SIAM Supplier in providing performance information in a defined, structured and rigorous way to facilitate automation of acquisition, exchange and quality management.
	2	**Manage Performance Information Quality**
06-02-03-003-01	3	The Hosting Supplier shall provide performance information to the Approved quality requirements as directed by the SIAM Supplier.

Requirement No.	Level	Requirement
		16. SERVICE LIFECYCLE MANAGEMENT
		16.1 Introduction
		16.1.1 The purpose of Service Lifecycle Management is to provide the tools and mechanisms to coordinate and control FITS Services and processes, from end to end, to manage the full lifecycle of FITS Services.
		16.2 IT Service Management Toolset
		16.2.1 The central requirement for the ITSM toolset is to ensure that there is a single source of authoritative information on any given Service Event and that the management of these events, to a successful conclusion, is available, visible, reportable and auditable from one source. The requirements listed below set out the obligations and relationship between the Suppliers in the selection, provision and operation of an end to end ITSM toolset solution.
		16.2.2 The ITSM toolset shall provide a common cross supplier interface for the management and support to all Hosting functions and processes and ensure that all Suppliers and the Authority have access to clear, accurate, timely and unambiguous information on the state, performance and operation of FITS Services provided to the Authority.

Requirement No.	Level	Requirement
		16.2.3 Access to and management of information is a core requirement in any process management role and having an integrated ITSM toolset in support the Service Delivery Lifecycle shall ensure that FITS Suppliers and the Authority can access the timely, informed and accurate information to enable the right discussions to be taken for the right reasons in a timely and effective manner.
		16.2.4 The ITSM toolset solution will be compliant with the ITIL Software Scheme as referenced in schedule 2.3 (Standards).
		16.2.5 The Service Requirements for ITSM toolset are listed in the below and further functional and non-functional requirements:
	2	**General Requirements**

Requirement No.	Level	Requirement
07-01-01-002-01	3	The Hosting Supplier shall utilise the ITSM toolset provided by the SIAM Supplier for the management of Service Events across the Service Delivery Lifecycle (SDLC). The use of the SIAM provided ITSM toolset is required to ensure the delivery of the following SIAM core processes: (i) Service Desk operation; (ii) Incident Management; (iii) Problem Management; (iv) Change and Evaluation Management; (v) Release and Deployment Management; (vi) Knowledge Management; and (vii) Request Fulfilment (including Access Management).
07-01-01-003-02	3	NOT USED
07-01-01-003-03 (Common)	3	The Hosting Supplier shall ensure that discovery and audit tools deployed in their ICT Environments are configured to deliver data discovery aligned to the concepts and relationships defined within the ICT Data Model.
07-01-01-003-11	3	The Hosting Supplier shall request via the FITS Service Catalogue, training in the use of the WAN and LAN Supplier's tooling.
07-01-01-004-03 (Common)	3	NOT USED
07-01-01-004-04	3	The Hosting Supplier shall request via the FITS Service Catalogue, training in the use of the Network Supplier's Tooling

Requirement No.	Level	Requirement
07-01-01-008-01	3	The Hosting Supplier shall either utilise or integrate with the ITSM toolset provided by the SIAM Supplier for the management of Service Events across the Service Delivery Lifecycle (SDLC). Toolset integration will be permitted across the following non-core processes: (i) Service Catalogue Management; (ii) Service Asset and Configuration Management (including Dependency & Discovery tools); (iii) Capacity Management; (iv) Availability Management; (v) Service Level Management; (vi) Event Management; (vii) Continual Service Improvement; (viii) Demand Management; (ix) Service Validation and Testing; and (x) Financial Management.
07-01-01-015-01	3	The Hosting Supplier shall ensure attendance at the SIAM Supplier's ITSM Toolset Training courses prior to the Hosting Supplier's Service Commencement Date to enable the Hosting Supplier to then provide ongoing training and support to their own personnel and ensure that they are suitably skilled to utilise the ITSM Toolset, in accordance with the ITSM Toolset Policy, Processes and Procedures.
07-01-01-023-01	3	The Hosting Supplier shall at all times, comply with the SIAM Supplier’s ITSM Toolset Policies, Processes and Procedures.

Requirement No.	Level	Requirement
		16.3 Architecture Management
		16.3.1 This encapsulates the following areas of Enterprise Architecture Management, Solution Architecture Management and Deployed Architecture Management to provide:
		(a) Vision & Strategy definition;
		(b) Architecture rules management (creation and maintenance of architecture and technology principles, policies, standards and reference models);
		(c) Architecture specification (business, information systems & information technology);
		(d) Improvement planning (opportunities, solutions, migration & transformation);
		(e) Realisation (including acquisition and implementation governance);
		(f) Architecture governance (architecture change management & requirements management); and
		(g) Architecture compliance and alignment monitoring.
		16.3.2 The purpose of Enterprise Architecture Management is to support the translation of the Authority's business vision and strategies into effective enterprise change; and to ensure the continuing alignment of IS/IT services provision to the Authority's business objectives.

Requirement No.	Level	Requirement
		16.3.3 The purpose of Solution Architecture Management is to support the delivery of specific change projects; to review architecture decisions and migration plans to identify efficiencies and advance standardisation; to ensure the solutions align to the architecture and technology principles, policies, standards and reference models defined by Enterprise Architecture Management processes; and capture and manage exceptions.
		16.3.4 The purpose of Deployed Architecture Management is to provide an up to date, consistent baseline of information about the provision of the End to End Services; to contribute to the integrated change planning process from demand to delivery; and to ensure compliance with and alignment to the Authority's Enterprise Architecture. Deployed Architecture Management facilitates alignment of the Deployed Architecture with Authority business objectives and operating models.
		16.3.5 The Service Requirements for Architecture Management are listed below:
	2	**Enterprise Architecture Management**
07-02-01-001-03 (Common)	3	The Hosting Supplier shall ensure that the provided Hosting Services Enterprise Architecture service is compliant with the Authority's Enterprise Architecture Policy, Processes and Procedures.
07-02-01-020-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier and the Other Suppliers as identified in the Dependencies Register to collate their aspects of the FITS Service Deployed Architecture Standards and Patterns.
07-02-01-023-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier and the Other Suppliers as identified in the Dependencies Register to collate their aspects of the FITS Service Deployed Architecture Roadmap.
	2	**Deployed Architecture Management**

Requirement No.	Level	Requirement
07-02-02-001-03 (Common)	3	NOT USED
07-02-02-002-03 (Common)	3	The Hosting Supplier shall provide Architecture Artefacts to describe the Hosting Services Deployed Architecture in accordance with the Authority's Architecture Governance Policy, Processes and Procedures and make them available through the SKMS within three (3) months of the Service Commencement Date.
07-02-02-003-03 (Common)	3	The Hosting Supplier shall update and maintain the Architecture Artefacts to describe the Hosting Services Deployed Architecture in accordance with the Authority's Architecture Governance Policy, Processes and Procedures not less than annually following the Service Commencement Date, and make the updates available through the SKMS within one (1) working day of the update being Approved.
07-02-02-004-03 (Common)	3	Not used
07-02-02-005-03 (Common)	3	NOT USED
07-02-02-006-03 (Common)	3	The Hosting Supplier shall provide the Hosting Services Deployed Architecture Standards and Patterns in accordance with the Authority's Architecture Governance Policy, Processes and Procedures and submit this to the Authority twice per year by January 1st and July 1st to decide Approval.
07-02-02-007-03 (Common)	3	NOT USED
07-02-02-008-03 (Common)	3	Not used
07-02-02-009-03 (Common)	3	NOT USED
07-02-02-010-03 (Common)	3	The Hosting Supplier shall perform Architecture Impact Assessment upon the Hosting Services Deployed Architecture to ensure ongoing manageability and supportability of the live environment, in accordance with the Authority's Architecture Governance Policy, Processes and Procedures.

Requirement No.	Level	Requirement
07-02-02-029-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier and the Other Suppliers as identified in the Dependencies Register to collate their aspects of the FITS Service Deployed Architecture Views.
07-02-02-037-01	3	The Hosting Supplier shall update the Approved Hosting Services Deployed Architecture Standards and Patterns in accordance with the Authority's Architecture Governance Policy, Processes and Procedures not less than quarterly, and make it available to the SIAM Supplier.
07-02-02-038-01	3	Not used
07-02-02-039-01	3	Not used
07-02-02-040-01	3	The Hosting Supplier shall ensure that the provided Hosting Services Deployed Architecture service is compliant with the SIAM Supplier's Deployed Architecture Policies, Processes and Procedures.
	2	**Solution Architecture Management**
07-02-03-001-03 (Common)	3	The Hosting Supplier shall ensure that the provided Hosting Services Solution Architecture service is compliant with the Authority's Solution Architecture Policy, Processes and Procedures.
07-02-03-002-03 (Common)	3	The Hosting Supplier shall, at the request of the Authority, provide input to the production and assessment of Architecture requirements and solution options, providing technical input into solution estimation.
07-02-03-003-03 (Common)	3	The Hosting Supplier shall, at the request of the Authority, provide input to the production of Solution Architectures that cover the domains of all relevant FITS Suppliers and those specific to Hosting Services. Solution Architectures shall include assessment and recommendation of the most appropriate implementation and migration planning approach.
	2	**Architecture Governance**
07-02-04-001-03 (Common)	3	The Hosting Supplier shall ensure that the provided Hosting Services Architecture Governance service is compliant with the Authority's Architecture Governance Policy, Processes and Procedures.

Requirement No.	Level	Requirement
07-02-04-002-03 (Common)	3	The Hosting Supplier shall participate in all relevant Architecture Governance activities and forums, as described in the Authority's Architecture Governance Policy, Processes and Procedures. The activities and forums of Architecture Governance will address all aspects of architecture delivery, including but not limited to; i) Enterprise Architecture Governance ii) Solution Architecture Governance iii) Deployed Architecture Governance
07-02-04-003-03 (Common)	3	NOT USED
07-02-04-004-03 (Common)	3	The Hosting Supplier shall ensure that all Approved Hosting Services Architecture Artefacts comply with the Architecture Content Framework and are made available through the SKMS, in accordance with the Authority's Architecture Governance Policy, Processes and Procedures.
07-02-04-005-03 (Common)	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to ensure that any Approved architectural dispensations, waivers, risks, issues and assumptions assigned to the Hosting Supplier are managed in accordance with the Authority's Architecture Governance Policy, Processes and Procedures.
07-02-04-006-03 (Common)	3	The Hosting Supplier shall work and collaborate with the Authority in the ongoing assessment and development of the Architecture Management capability of the FITS Service.
07-02-04-007-03 (Common)	3	The Hosting Supplier shall provide Architectural leadership in relation to Hosting Services, providing strategy and direction to the Authority, Other Suppliers as identified in the Dependencies Register and on the request of the Authority, to other Stakeholders.
07-02-04-008-03 (Common)	3	The Hosting Supplier shall provide and maintain a catalogue service that the Authority can request to provide architectural expertise in the Architecture of Hosting Services or other Architecture domains. The expertise shall align to the Skills Framework for the Information Age (SFIA) version 5 or later.

Requirement No.	Level	Requirement
07-02-04-021-01	3	The Hosting Supplier shall comply with the consolidated FITS Service Deployed Architecture Standards and Patterns, collated by the SIAM Supplier, when providing services to be hosted within the ICT Environments of Other FITS Suppliers, unless otherwise agreed by the Authority.
	2	**Innovation Management**
07-02-05-001-03 (Common)	3	Not used
07-02-05-002-03	3	Not used

Requirement No.	Level	Requirement
		16.4 Application Performance Management
		16.4.1 The Authority requires the ability to manage the performance of Business Applications. The requirements for this service need to accommodate for all stages of the Application lifecycle:
		(a) Design;
		(b) Implement;
		(c) Monitor;
		(d) Report; and
		(e) Act.
		16.4.2 The principle objective of Application Performance Management is to maintain an appropriate level of performance and availability for a defined set of Business Applications by continuously monitoring and measuring their performance and promptly identifying any potential issue.
		16.4.3 The Service Requirements for Application Performance Monitoring (APM) are listed below:
	2	**Application Performance Measurement**
07-03-01-008-01	3	The Hosting Supplier shall support, where required, the SIAM Supplier in the appropriate implementation of the APM Service and its associated tools across the relevant components for which they have responsibility.
07-03-01-011-01	3	The Hosting Supplier shall support, where required, the SIAM Supplier in measuring the performance of designated Business Applications in accordance with the Service Levels set out in schedule 2.2 (Service Performance Management).

Requirement No.	Level	Requirement
	2	**Change Management**
	3	Not applicable
	2	**Future Services**
07-03-03-003-01	3	The Hosting Supplier shall support the SIAM Supplier in planning the base lining and subsequent Performance monitoring, for the Services they provide, for any future Business Application, at the request of the SIAM Supplier.
07-03-03-006-01	3	The Hosting Supplier shall support the SIAM Supplier to provide the plan for, and implementation of, a fast track monitoring service for Business Applications.
		16.5 Licence Management and Compliance
		16.5.1 The requirements set out in this section refer to the obligations on the Hosting Supplier with regards to adherence to Software licensing terms and conditions for the Hosting Services consumed by the Authority.
		16.5.2 The Service Requirements for Licence Management and Compliance are listed below:
	2	**General Requirements**
07-04-01-001-03	3	The Hosting Supplier shall comply with the Authority's Software Licensing Policy.
07-04-01-002-03	3	The Hosting Supplier, where required by the Authority, shall manage the procurement of Licences and Licence renewals in accordance with the Authority's Software Licensing Policy.
07-04-01-003-03	3	The Hosting Supplier shall be responsible for ensuring that suitable licence arrangements are in place for all Software utilised by the Hosting Services in accordance with the Authority's Software Licensing Policy.

Requirement No.	Level	Requirement
07-04-01-005-01	3	The Hosting Supplier shall allow the SIAM Supplier to request the installation and configuration of tools for the purpose of monitoring the presence of unauthorised or unlicensed Software.
07-04-01-005-03	3	NOT USED
07-04-01-006-03	3	The Hosting Supplier shall be responsible for the ongoing management and monitoring of licence usage, within the Hosting Services, in order to ensure that such usage is both legal and efficient, including the enablement of licence re-deployment to minimise licence costs.
07-04-01-007-01	3	The Hosting Supplier shall capture, manage and monitor licence usage and ensure updates to the CMDB are performed in accordance with the SIAM Supplier's SACM Policies, Processes and Procedures and within the Service Levels set out in schedule 2.2 (Service Performance Management).
07-04-01-007-03	3	The Hosting Supplier shall check the Software licence availability in the CMDB and re-use or upgrade any suitable license(s).
07-04-01-008-01	3	The Hosting Supplier shall provide evidence as requested by the SIAM Supplier on the status of all licensing for Software they use in delivering the Hosting Service, within five (5) Working Days of such a request.
07-04-01-008-03	3	The Hosting Supplier shall, where the CMDB contains no available licence, procure such additional licences as necessary in accordance with the Authority's Software Licensing Policy.
07-04-01-009-03	3	NOT USED

Requirement No.	Level	Requirement
		16.6 Value Add Services
		16.6.1 These Service Requirements are designed to offer additional services which the Authority may contract for where the Hosting Supplier can demonstrate value for money.
		16.6.2 The Service Requirements for Value Add Services are listed below:
	2	**Strategy Generation**
07-05-01-001-03	3	The Hosting Supplier shall provide Hosting Service expertise and support the Authority in its generation of its ICT Strategy.
	2	**Strategy Implementation**
07-05-02-006-01	3	The Hosting Supplier shall support the SIAM Supplier to provide the Authority with a model of the future state Architecture based on the future state Project pipeline.
	2	**Financial Management**
	3	Not applicable
	2	**Portfolio Management**
	3	Not applicable
	2	**Service Portfolio Management**
	3	Not applicable
	2	**Demand Management**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Supplier Management**
	3	Not applicable
	2	**Requirements Analysis**
	3	Not applicable
	2	**Coordination and Delivery**
	3	Not applicable
	2	**Innovation**
07-05-10-001-03	3	The Hosting Supplier shall provide innovation proposals with supporting business cases to the Authority for the Hosting Services in accordance with the section 8 of the MSA.
	2	**Local Server Room Facilities Management**
	3	Not applicable
	2	**WAN and LAN Services Procurement**
	3	Not applicable
	2	**Enhanced Conferencing Services**
	3	Not applicable
	2	**Extended Voice Mail**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Operator Services**
	3	Not applicable
	2	**High Security Telephony Services**
	3	Not applicable

Requirement No.	Level	Requirement
		17. INFORMATION SECURITY MANAGEMENT
		17.1.1 The purpose of Information Security Management is to:
		(a) Align ICT security with business security and ensure that information security is effective for all FITS Services and Service Management activities;
		(b) Ensure the confidentiality, integrity and availability of the Authority's information, data and FITS Services;
		(c) Ensure compliance with the Authority Accreditation obligation; and
		(d) Ensure alignment with the HMG Security Policy Framework and associated information assurance standards.
		17.1.2 Information Security Management shall ensure the Authority's Information Security Policy is enforced and maintained by a set of detailed requirements which cover the following categories:
		(a) Security Policy and Standards;
		(b) Security Awareness;
		(c) Vulnerability Management;
		(d) Security Incident Management;
		(e) Accreditation Management;
		(f) Security Assurance;

Requirement No.	Level	Requirement
		(g) Information Security Audit;
		(h) Protective Monitoring;
		(i) IT Health Checks;
		(j) Digital Forensics;
		(k) Connection Criteria; and
		(l) Information Security Risk Management.
		17.2 Security Policy and Standard
		17.2.1 These requirements set out the obligations on the Supplier regarding the Development, maintenance and compliance with HM Government Security Policy Framework (SPF) statutory security and confidentiality laws and privacy policies.
		17.2.2 The Service Requirements for Security Policy and Standard Services are listed below:
	2	**General Requirements**
08-01-01-001-03 (Common)	3	The Hosting Supplier shall ensure that Hosting Services comply with the Authority's ICT Information Assurance (IA) Policies, Processes and Procedures.
08-01-01-002-03 (Common)	3	The Hosting Supplier shall ensure that all Sites containing Protectively Marked Assets, for which they are responsible, have physical security controls commensurate with the highest Protective Marking or classification of those assets as specified by the SPF. For sites where CONFIDENTIAL material is handled, ListX certification is mandatory. The Authority reserves the right to audit the physical security of any site storing or processing Protectively Marked information assets in support of FITS Services.

Requirement No.	Level	Requirement
08-01-01-004-01	3	The Hosting Supplier shall provide an impact assessment of changes to legal and regulatory requirements, HMG IA Strategies, Policies, Processes, Guidance and Standards on the Hosting Services to the SIAM Supplier within ten (10) Working Days of a request from SIAM.
08-01-01-009-01	3	The Hosting Supplier shall provide a report for each Service Reporting Period on the Hosting Supplier's compliance with the Authority's ICT Information Assurance (IA) Policies, Processes and Procedures and provide the report within five (5) Working Days of the end of the previous Service Reporting Period to the SIAM Supplier in a format as agreed with the SIAM Supplier.
		17.3 Security Awareness
		17.3.1 These requirements are to ensure all users are aware of, understand and formally accept their security responsibilities.
		17.3.2 The Service Requirements for Security Awareness Services are listed below:
	2	**Security education and training**
08-02-01-001-03 (Common)	3	The Hosting Supplier shall instigate a programme of security awareness, education and training for the Hosting Supplier's Personnel within twenty (20) days of the Effective Date.
08-02-01-002-03 (Common)	3	The Hosting Supplier shall ensure that the Hosting Supplier's Personnel have undertaken security awareness, education and training prior to using or supporting the Hosting Services and annually thereafter.
08-02-01-004-01	3	The Hosting Supplier shall develop and maintain security awareness material and training programmes applicable to the Hosting Services.
08-02-01-005-01	3	The Hosting Supplier shall maintain, review and update where necessary, the security awareness material and training programmes for Hosting Services at least annually.

Requirement No.	Level	Requirement
08-02-01-010-01	3	The Hosting Supplier shall provide a report for each Service Reporting Period on the status of their security awareness education & training programme and provide the report within five (5) Working Days of the end of the previous Service Reporting Period to the SIAM Supplier in a format as agreed with the SIAM Supplier.
		17.4 Vulnerability Management
		17.4.1 The Vulnerability Management service shall mitigate against threats and weaknesses that could lead to security incidents and take appropriate corrective action. Requirement will include:
		(a) Ensuring all systems and software are supported by vendor security fixes. The monitoring for vendor security alerts, assessment of criticality and implementation in accordance with the patching policy;
		(b) Ensuring that all systems are adequately protected from the threat of malicious code of all types. Keeping anti-virus and intrusion detection definitions and software up to date. Quarantining malware and alerts triggered on detection and the raising of security incidents when malware is detected; and
		(c) Ensuring that unauthorised devices are not connected to the networks or other ICT equipment. Authorised devices must be operated in accordance with security policies.
		17.4.2 The Service Requirements for Threat and Vulnerability Management Services are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
08-03-01-001-03 (Common)	3	The Hosting Supplier shall adhere to the Security Content Automation Protocol (SCAP) suite of specifications when measuring, scoring and describing vulnerabilities, including but not limited to: i) CVE (Common Vulnerabilities and Exposures) identifiers for publicly known information security vulnerabilities; ii) CVSS (Common Vulnerability Scoring System) for scoring and measuring information security vulnerabilities; and iii) CCSS (Common Configuration Scoring System) for scoring and measuring the severity of Software security configuration issues.
08-03-01-002-03 (Common)	3	NOT USED
08-03-01-009-01	3	The Hosting Supplier shall monitor Vulnerability Notices, from their vendors and the SIAM Vulnerability Management Service for all products and services in the ICT Environments provided by the Hosting Supplier and provide an impact assessment to the SIAM Supplier's Vulnerability Management Service within one (1) Working Day of the Vulnerability Notice being issued.
08-03-01-012-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in the production and implementation of Resolution Plans, carrying out any activities that affect the Hosting Supplier's Services in accordance with the Change and Evaluation Management Policies, Processes and Procedures.
08-03-01-015-01	3	The Hosting Supplier shall produce reports each Service Reporting Period on the Vulnerability Management Service for the Hosting Supplier's Services in a format to be agreed with the SIAM Supplier, and provide the report to the SIAM Supplier within five (5) Working Days of the end of the preceding Service Reporting Period.

Requirement No.	Level	Requirement
08-03-01-016-01	3	For every vulnerability the Hosting Supplier has conducted an impact assessment for using CVSS they shall work and collaborate with Other FITS Suppliers to develop a Vulnerability Resolution Plan to mitigate the vulnerability and publish the plan to the SIAM Supplier's Vulnerability Management Service within: (i) three (3) Working Days for vulnerabilities rated as high - CVSS score greater than or equal to seven (7); (ii) ten (10) Working Days for vulnerabilities rated as medium - CVSS score greater than or equal four (4) but less than seven (7); and (iii) fifteen (15) Working for vulnerabilities rated as low - CVSS score less than four (4)
	2	**Security Patch Management**
08-03-02-001-03 (Common)	3	The Hosting Supplier shall comply with the Authority's Security Patch Management Policies, Processes and Procedures.
08-03-02-002-01	3	The Hosting Supplier shall develop Security Patch Management Processes and Procedures for the Hosting Services, in accordance with the SIAM Supplier's Security Patch Management Policies and submit these to the Authority, within forty (40) Working Days prior to the Hosting Supplier's Service Commencement Date, to decide Approval.
08-03-02-005-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to maintain the Security Patch Management Policies, Processes and Procedures for Hosting Services.
08-03-02-008-01	3	The Hosting Supplier shall produce reports each Service Reporting Period detailing their compliance with the Security Patch Management Policies, Processes and Procedures in a format to be agreed with the SIAM Supplier, and provide the report to the SIAM Supplier within five (5) Working Days of the end of the preceding Service Reporting Period.
08-03-02-010-01	3	The Hosting Supplier shall work with the SIAM Supplier to produce Resolution Plans for non-compliance to the Security Patch Management Policies, Processes and Procedures.

Requirement No.	Level	Requirement
08-03-02-012-01	3	The Hosting Supplier shall cooperate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.
08-03-02-014-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.
	2	**Protection against Malicious Software**
08-03-03-001-03 (Common)	3	The Hosting Supplier shall provide and maintain Malicious Software protection for the Hosting Supplier's ICT Environment in accordance with the Authority's ICT Information Assurance (IA) Policies, Processes and Procedures.
08-03-03-002-03 (Common)	3	The Hosting Supplier shall ensure that updates for Malicious Software protection are distributed to and installed upon all Devices unless otherwise agreed to with the Authority within four (4) hours of public release of the updates and in accordance with the Change and Evaluation Management Policies, Processes and Procedures.
08-03-03-003-03 (Common)	3	The Hosting Suppliers shall install GovCertUK signatures and recommended configuration including but not limited to: (i) Attack Detection Signatures; (ii) Domain block lists; (iii) URL block lists; and (iv) IP block lists, to detect and prevent attacks known by GovCertUK to target UK HMG systems.
	2	**Device Control**

Requirement No.	Level	Requirement
	3	Not applicable
		17.5 Security Incident Management
		17.5.1 The initiation, management, resolution, mitigation and reporting of security incidents, in compliance with security incident management policy and procedures.
		17.5.2 The Service Requirements for Security Incident Management Services are listed below:
	2	**Identify and escalate security incidents**
08-04-01-001-03 (Common)	3	The Hosting Supplier shall comply with the processes and procedures for the identification and escalation of Security Incidents and associated Problems in accordance with the Authority's ICT Information Assurance (IA) Policies, Processes and Procedures and SIAM Supplier's Security Incident Management Policies, Processes and Procedures.
08-04-01-002-03 (Common)	3	The Hosting Supplier shall ensure that Security Alerts / Events are categorised by Severity / Priority level as defined in schedule 2.2 (Service Performance Management).
08-04-01-003-03 (Common)	3	NOT USED
08-04-01-004-01	3	The Hosting Supplier shall, on detection of a potential Security Incident affecting FITS ICT Environments, perform an initial investigation and work and collaborate with the SIAM Supplier to identify and categorise a Security Incident according to the Incident Severity and Priority definitions in schedule 2.2 (Service Performance Management).
08-04-01-006-01	3	The Hosting Supplier shall support the SIAM Supplier in developing a TOR for Security Investigations for Hosting Services.

Requirement No.	Level	Requirement
08-04-01-009-01	3	The Hosting Supplier shall work and collaborate with the Other Suppliers, as identified in the Dependencies Register and the Authority to produce the Security Incident Resolution Plan in the timescales specified in schedule 2.2 (Service Performance Management).
08-04-01-012-01	3	The Hosting Supplier shall provide reports each Service Reporting Period to the SIAM Supplier on identified or escalated Security Incidents and associated Problems within five (5) Working Days of the end of the preceding Service Reporting Period, in a format to be agreed with the SIAM.
08-04-01-016-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.
08-04-01-017-01	3	The Hosting Supplier shall, at the request of the SIAM Supplier, provide the SIAM Supplier or the Authority with legally authorised surveillance access to the Hosting Supplier's ICT systems and the Authority's data to assist in any investigation.
		17.6 Accreditation Management
		17.6.1 Accreditation Management is the management of the ongoing compliance with the HMG Information Security Standards, Security Policy Framework, and HMG IA guidance to achieve formal IA accreditation of FITS ICT systems.
		17.6.2 The Service Requirements for Accreditation Management Services are listed below:
	2	**General Requirements**
08-05-01-001-03 (Common)	3	The Hosting Supplier shall produce information risk management documentation, including RMADS, Compliance Statements against the Security Controls Objectives Matrix and other associated evidence supporting Security Accreditation of the Hosting Services, in accordance with the Authority's Accreditation Strategy and Accreditation Frameworks.

Requirement No.	Level	Requirement
08-05-01-002-03 (Common)	3	The Hosting Supplier shall produce and maintain RMADS and supporting documentary evidence for the Hosting Services in accordance with the Authority Accreditation Strategy and Authority Accreditation Frameworks and enable the Authority to make an initial Accreditation decision before the Service Commencement Date.
08-05-01-003-03 (Common)	3	The Hosting Supplier shall produce and maintain Risk Treatment Plans, Security Cases and SecCOM Compliance Statements in respect of the risks identified in the HMG IAS1&2 Supplement Risk Assessments and Organisational Risk Assessment for the Hosting Services in accordance with the timescales agreed in the Security Management Plan.
08-05-01-004-03 (Common)	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to seek Authority Approval of Risk Treatment Plans, Security Cases and SecCOM Compliance Statements in respect of any of the Hosting Services in accordance with the timescales agreed in the Security Management Plan.
08-05-01-005-03 (Common)	3	The Hosting Supplier shall implement the Approved Risk Treatment Plans in accordance with the Change and Evaluation Management Policies, Processes and Procedures.
08-05-01-009-01	3	The Hosting Supplier shall complete a review of the RMADS and supporting documentation for which they are responsible and provide updates, where necessary, to the Security Accreditor and the SIAM Supplier within two (2) months prior to the expiry of the previous successful accreditation for Approval.
08-05-01-012-01	3	The Hosting Supplier shall, if a significant change (as determined by the Authority) to the Hosting Services has occurred, complete a review of the Hosting Services of Threats and Risks to the systems for which they are responsible and provide the review to the SIAM Supplier within one (1) month of the significant change.

Requirement No.	Level	Requirement
		17.7 Security Assurance
		17.7.1 The ensurance that all security controls, whether technical, physical or procedural, are compliant with security policy and are compliant with the appropriate assurance requirements.
		17.7.2 The Service Requirements for Security Assurance Services are listed below:
	2	**Compliance and Assurance**
08-06-01-001-03 (Common)	3	The Hosting Supplier shall ensure their Services are Accredited to handle the appropriate Business Impact Levels and Protective Markings associated within communicating, storing, transferring and processing data by their Services by the Service Commencement Date.
08-06-01-002-03 (Common)	3	The Hosting Supplier shall, where it is required to store cryptographic material in the provision of their Services, provide an authorised custodian to protect the cryptographic material in accordance with HMG IAS4.
08-06-01-003-01	3	The Hosting Supplier shall produce a report every three (3) Service Reporting Periods detailing their compliance to schedule 2.5 (Security Management Plan), and provide this report to the SIAM Supplier within five (5) Working Days of the end of the preceding three (3) Service Reporting Periods.
08-06-01-005-01	3	The Hosting Supplier shall support the Authority and the SIAM Supplier in the process of the storage, deployment, renewal, disposal and accounting for controlled cryptographic material in accordance with the HMG Security Policy Framework and the Standards provided by the Authority.

Requirement No.	Level	Requirement
		17.8 Information Security Audit
		17.8.1 Covers the identification of the specific criteria against which a security audit will be conducted, the need to ensure that the services are operated in accordance with all security policies, procedures and requirements and the provision of evidence of compliance in the event of an audit.
		17.8.2 The Service Requirements for Information Security Audit Services are listed below:
	2	**General Requirements**
08-07-01-001-03 (Common)	3	The Hosting Supplier shall comply with the Authority's Information Security Audit Policies, Processes, Procedures and compliance criteria.
08-07-01-002-03 (Common)	3	The Hosting Supplier shall allow access for the Authority to conduct an Information Security Audit at any time. The Authority will give reasonable notice for such audits where possible, but reserves the right to conduct such audits without notice when necessary.
08-07-01-005-01	3	The Hosting Supplier shall conduct Information Security Audits in line with the Authority's Information Security Audit Policies, Processes and Procedures and compliance criteria for the Services they provide and report compliance status to the SIAM Supplier within one (1) month of the anniversary of the Hosting Supplier's Effective Date.
08-07-01-007-01	3	The Hosting Supplier shall produce a Resolution Plan with remediation timescales in accordance with the Authority Information Risk Policy Guidance, for Hosting Services which are shown to be non compliant by an Information Security Audit. The Supplier shall provide this plan to the SIAM Supplier within ten (10) Working Days of receipt of their Information Security Audit report.
08-07-01-009-01	3	The Hosting Supplier shall cooperate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.

Requirement No.	Level	Requirement
08-07-01-011-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.
	2	**Monitor and Manage Compliance**
08-07-02-002-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to ensure compliance with the Authority's Information Security Audit Policies, Processes and Procedures and compliance criteria.
08-07-02-004-01	3	The Hosting Supplier shall provide to the SIAM Supplier reporting information for the IAMM in a format to be agreed with the SIAM Supplier on an annual basis with the date to be agreed with the SIAM Supplier.
		17.9 Protective Monitoring
		17.9.1 The implementation of technology to enable network monitoring as directed by the Security Tower Supplier. The provision to the Security Services tower provider of the relevant system log files and alerts to enable an effective protective monitoring service in compliance with good practice guide 13.
		17.9.2 The Service Requirements for Protective Monitoring Services are listed below:
	2	**General Requirements**
08-08-01-002-01	3	The Hosting Supplier shall support the SIAM Supplier and the Specialist Security Services Suppliers to deliver Protective Monitoring.

Requirement No.	Level	Requirement
08-08-01-006-08	3	The Hosting Supplier shall host Devices and Software provided and managed by the Protective Monitoring Supplier including but not limited to: i) NIDS; ii) Passive Network Taps; iii) management servers; iv) switches; v) firewalls; and vi) routers; in support of the Protective Monitoring Service.
08-08-01-008-08	3	The Hosting Supplier shall supply the SIAM Supplier with detailed logical and physical network diagrams that shall include details of all Configuration Items including but not limited to: i) all Devices including type (including but not limited to: workstation; server; switch; router; firewall); ii) layer 2 VLAN information; iii) layer 3 IP subnet, routing and address information; and iv) protocol flows. These diagrams shall be issued by the Service Commencement Date for Hosting Service. Should any Changes affect the accuracy of these diagrams, they shall be updated and re-issued within twenty (20) Working Days of that Change.

Requirement No.	Level	Requirement
08-08-01-021-08	3	The Hosting Supplier shall ensure that no data in scope for Payment Card Industry Data Security Standard (PCI DSS) compliance is sent to the Protective Monitoring Supplier.
08-08-01-024-08	3	The Hosting Supplier shall adhere to the Security Content Automation Protocol (SCAP) suite of specifications when measuring, scoring and describing vulnerabilities, including but not limited to: i) CVE (Common Vulnerabilities and Exposures) identifiers for publicly known information security vulnerabilities; ii) CVSS (Common Vulnerability Scoring System) for scoring and measuring information security vulnerabilities; and iii) CCSS (Common Configuration Scoring System) for scoring and measuring the severity of Software security configuration issues.
	2	**Protective Monitoring Policy**
08-08-02-006-08	3	The Hosting Supplier shall produce a Protective Monitoring Policy for the Hosting Supplier ICT Environment within the standard template issued by the SIAM Supplier and following the process and timescales detailed in the Authority Accreditation Framework.
08-08-02-009-08	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to review the Protective Monitoring Policy for the Hosting Supplier ICT Environments in scope of that policy and provide review comments to the SIAM Supplier within five (5) Working Days of receipt.
	2	**Protective Monitoring Service Configuration**
08-08-03-003-08	3	The Hosting Supplier shall ensure that Protective Monitoring Accounting Items for all Protectively Monitored Devices and Protectively Monitored Software are generated, captured and delivered to the Protective Monitoring Supplier.

Requirement No.	Level	Requirement
08-08-03-010-08	3	The Hosting Supplier shall install and configure the HIDS and Log Collection Software provided by the Protective Monitoring Supplier within the timescales agreed in the Implementation Plan or no later than thirty (30) Working Days following the Authority request. The Hosting Supplier shall provision this Software as part of solutions to support the delivery of Hosting Services and confirm within six (6) months of the Service Commencement Date.
08-08-03-013-08	3	The Hosting Supplier shall work and collaborate with the Protective Monitoring Supplier for the purpose of connecting network monitoring or network IDS components to the Hosting Supplier ICT Environment, including but not limited to deployment of Passive Network Taps.
08-08-03-019-08	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to review the PMC Config document for the Hosting Supplier's ICT Environment in scope of the PMC Config document.
	2	**Protective Monitoring Accounting**
08-08-04-003-08	3	The Hosting Supplier shall perform log management tasks for Devices and Configuration Items including but not limited to configuring and managing: i) log retention; ii) log rotation; and iii) log generation.
08-08-04-004-08	3	The Hosting Supplier shall ensure that the inbuilt event log management facilities of the underlying Operating System of Protectively Monitored Devices is used to manage the Operating System event logs, unless otherwise agreed with the Authority.

Requirement No.	Level	Requirement
08-08-04-015-08	3	The Hosting Supplier shall adhere to the Accounting Log format provided by the Protective Monitoring Supplier for any Specially Written Software which they produce, manage or maintain.
08-08-04-029-08	3	The Hosting Supplier shall use Manual Accounting Processes to supplement the Protective Monitoring Service as agreed with the Authority.
	2	**Protective Monitoring - Monitoring and Auditing**
	3	Not applicable
	2	**Protective Monitoring Tuning**
08-08-06-002-08	3	The Hosting Supplier will support the Protective Monitoring Supplier in performing tuning across the Protective Monitoring Service to reduce the number of false positive and false negative alerts and to optimise the collection and processing of Accounting Data.
	2	**Protective Monitoring Reporting**
08-08-07-004-08	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to review and analyse Protective Monitoring reports and agree follow on actions for their respective Services within ten (10) Working Days of receipt.
	2	**Protective Monitoring Incident Management**
	3	Not applicable

Requirement No.	Level	Requirement
	2	**Protective Monitoring Remediation**
08-08-09-003-08	3	The Hosting Supplier shall work and collaborate with the Other Suppliers and the Authority to produce the Protective Monitoring Resolution Plan in the timescales agreed with the Authority.
08-08-09-008-08	3	The Hosting Supplier shall implement the Approved Protective Monitoring Resolution Plan.
		17.10 IT Health Check
		17.10.1 To ensure the correct implementation of security functionality and to identify vulnerabilities in IT systems and networks, which may compromise confidentiality, integrity or availability of information on the systems or networks.
		17.10.2 The Service Requirements for the IT Health Check Services are listed below:
	2	**General requirements**
08-09-01-002-01	3	The Hosting Supplier shall support the SIAM Supplier and the Specialist Security Services Suppliers to deliver IT Health Checks.
	2	**CHECK Team**
	3	Not applicable
	2	**CHECK Strategy**
08-09-03-004-06	3	The Hosting Supplier shall review the Authority's CHECK Testing Strategy and send review comments to the SIAM Supplier within twenty (20) Working Days of receipt of the CHECK Testing Strategy.

Requirement No.	Level	Requirement
08-09-03-010-06	3	The Hosting Supplier shall review the Authority's CHECK Testing Roadmap and send review comments to the SIAM Supplier within twenty (20) Working Days of receipt.
	2	**CHECK Scoping**
08-09-04-002-06	3	The Hosting Supplier shall notify the SIAM Supplier of a CHECK Test request via the Service Catalogue.
08-09-04-006-06	3	The Hosting Supplier shall, at the request of the SIAM Supplier, work and collaborate with the Other Suppliers, as identified in the Dependencies Register, and the SIAM Supplier to produce the CHECK Test Statement of Requirements for their respective Check Test request within ten (10) Working Days of receipt of such documentation.
	2	**CHECK Testing**
08-09-05-006-06	3	The Hosting Supplier shall conduct activities required to support the CHECK Test as specified in the CHECK Scope, including but not limited to: i) escorting CHECK team members; ii) arranging access to Authority Sites; iii) providing required documentation; iv) implement required system changes; and v) manage user accounts
	2	**CHECK Reporting**
	3	Not applicable
	2	**CHECK Remediation**

Requirement No.	Level	Requirement
08-09-07-001-06	3	On receipt of the CHECK Report, the Hosting Supplier and Other Authority Providers shall work and collaborate with each other and the SIAM Supplier to produce the IT Health CHECK Resolution Plan for each individual finding in the CHECK Report within: i) three (3) Working Days for vulnerabilities rated as high - CVSS score greater than or equal to seven (7); ii) ten (10) Working Days for vulnerabilities rated as medium - CVSS score greater than or equal four (4) but less than seven (7); and iii) fifteen (15) Working Days for vulnerabilities rated as low - CVSS score less than four (4).
08-09-07-007-06	3	The Hosting Supplier shall implement the Approved CHECK Resolution Plan.
		17.11 Digital Forensics
		17.11.1 The process of uncovering and interpreting electronic data whilst preserving evidence in its most original form, to support a structured investigation by collecting and identifying and validating the digital information for the purpose of reconstruction past events.
		17.11.2 The Service Requirements for Digital Forensics Services are listed below:
	2	**General requirements**
08-10-01-002-01	3	The Hosting Supplier shall support the SIAM Supplier and the Specialist Security Services Suppliers to deliver Digital Forensics.
08-10-01-006-07	3	The Hosting Supplier shall adhere to CESG Good Practice Guide 18 and CESG Implementation Guide 18 with regard to Forensic Readiness Policies and Forensic Readiness planning.
	2	**Digital Forensic Consultancy**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Digital Forensic Readiness Policy**
	3	Not applicable
	2	**Digital Forensic Training**
08-10-04-007-07	3	The Hosting Supplier shall deliver Digital Forensic training material distributed by the SIAM Supplier and produced by the Digital Forensics Supplier to all Hosting Supplier Personnel within forty (40) Working Days of their Effective Date.
08-10-04-009-07	3	The Hosting Supplier shall ensure that the Digital Forensic training material distributed by the SIAM Supplier and produced by the Digital Forensics Supplier is delivered to all Hosting Supplier Personnel within fifteen (15) Working Days of the start of their employment term on the FITS Agreement and annually thereafter.
	2	**Digital Forensic Planning**
08-10-05-004-07	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to make a recommendation to the Authority on the requirement for a Forensic Readiness Plan following the process and timescales detailed in the Authority Accreditation Framework.
08-10-05-009-07	3	The Hosting Supplier shall produce Forensic Readiness Plans in accordance with the Authority's Forensic Readiness Policy and send to the SIAM Supplier within twenty (20) Working Days of the Authority approving the requirement for a Forensic Readiness Plan.
	2	**Digital Forensic Incident Management**
08-10-06-005-07	3	The Hosting Supplier shall adhere to the SIAM-managed process for initiating a Digital Forensic Investigation.

Requirement No.	Level	Requirement
	2	**Digital Forensic Investigations**
08-10-07-002-07	3	The Hosting Supplier shall support the SIAM Supplier in developing Terms of Reference (ToR) for Digital Forensic Investigations for the Hosting Services within: i) one (1) Working Day for Severity one (1) incidents; ii) three (3) Working Days for Severity two (2) incidents; and iii) five (5) Working Days for Severity three (3) incidents.
08-10-07-011-07	3	The Hosting Supplier shall provide support to Approved Digital Forensic Investigations, including but not limited to access to: i) Authority Sites; ii) Suppliers' Sites; iii) documentation; and iv) technical specialists.
	2	**Digital Forensic Reporting**
08-10-08-004-07	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier to review and agree the Digital Forensic reports within five (5) Working Days of receipt of the Digital Forensic Report from the Digital Forensics Supplier and send to the Authority for Approval.
	2	**Digital Forensic Remediation**

Requirement No.	Level	Requirement
08-10-09-002-07	3	On receipt of the Digital Forensic report from the SIAM Supplier, the Hosting Supplier shall develop for Approval a Digital Forensic Resolution Plan for each individual finding in the Digital Forensic Report within: i) three (3) Working Days for vulnerabilities rated as high - CVSS score greater than or equal to seven (7); ii) ten (10) Working Days for vulnerabilities rated as medium - CVSS score greater than or equal four (4) but less than seven (7); and iii) fifteen (15) Working Days for vulnerabilities rated as low - CVSS score less than four (4).
08-10-09-007-07	3	The Hosting Supplier shall implement the Approved Digital Forensics Resolution Plans.
		17.12 Connection Criteria
		17.12.1 Connection Criteria shall ensure compliance with any applicable third party agreement for connecting networks.
		17.12.2 The Service Requirements for Connection Criteria are listed below:
	2	**Compliance**
08-11-01-002-01	3	The Hosting Supplier shall, for all Connections used in the provision of the Hosting Services, operate those Connections in compliance with the relevant Connection Criteria and produce and maintain in line with the obligations documented in the Connection Criteria.
08-11-01-003-01	3	The Hosting Supplier shall, for all Connections used in the provision of the Hosting Services, produce and maintain and provide to the SIAM Supplier compliance statements and supporting documentary evidence in line with the obligations documented in the Connection Criteria.

Requirement No.	Level	Requirement
08-11-01-006-01	3	The Hosting Supplier shall, for the FITS Services they provide, alert the SIAM Supplier within one (1) working day where any Connection is non-compliant with its Connection Criteria and work with the SIAM Supplier to produce appropriate Resolution Plans.
08-11-01-008-01	3	The Hosting Supplier shall, for any non-compliant Connections within the FITS Services they provide, work and collaborate with the SIAM Supplier to implement the Approved Resolution Plans within the agreed timescales.
		17.13 Information Security Risk Management
		17.13.1 Information Security Risk Management covers integration of Information Security Management with the wider Risk Management service. It provides the reporting structure, escalation paths and Stakeholder communication between Information Security Management service and Risk Management.
		17.13.2 The Service Requirements for Information Security Risk Management are listed below:
	2	**General requirements**
08-12-01-001-01	3	The Hosting Supplier shall comply with the Authority's Information Security Risk Management Policies and the SIAM Supplier's Information Security Risk Management Processes and Procedures.
08-12-01-002-01	3	The Hosting Supplier shall work and collaborate with the SIAM Supplier in any review as a result of the Hosting Supplier’s non-compliance with the Authority's Information Security Risk Management Policies or the SIAM Supplier's Information Security Risk Management Processes and Procedures and implement any required corrective action.

Requirement No.	Level	Requirement
		18. END USER SERVICES
		18.1 End User Device
		18.1.1 The provision of devices to End Users to support them in their business roles, the environment(s) in which they are operating and the data or systems with which they will be interacting.
		18.1.2 The Service Requirements for End User Device Services are listed below:
	2	**Client Devices**
	3	Not applicable
	2	**Mobile Client Devices**
	3	Not applicable
	2	**Client Builds**
09-01-03-002-02	3	The Hosting Supplier shall work and collaborate with the Authority, Other Suppliers as identified in the Dependencies Register and Other Authority Providers where appropriate to agree the components they require included in the Client Builds in order to deliver the EUCS Supplier's components of the End to End Services.
	2	**Peripheral Equipment**
	3	Not applicable

Requirement No.	Level	Requirement
		18.2 Presentation and Provisioning
		18.2.1 This covers both the Client presentation, the customisation and look and feel of the client user interface, and the delivery of Client Software and Applications to a Client Device.
		18.2.2 The Service Requirements for Presentation and Provisioning are listed below:
	2	**Client Presentation and Personalisation**
09-02-01-010-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier to ensure that End Users are able to access the FITS Services via Client Devices.
	2	**Provision of Client Software and Business Applications**
	3	Not applicable
		18.3 Telephony Devices
		18.3.1 Telephone devices for the use of end users.
		18.3.2 The Service Requirements for Telephony Devices are listed below:
	2	**Fixed Telephony Devices**
	3	Not applicable
	2	**Mobile Telephony Devices**
	3	Not applicable

OFFICIAL

Requirement No.	Level	Requirement
	2	**Pager Devices**
	3	Not applicable
		18.4 Document Copy and Print
		18.4.1 Printing, scanning, and facsimile services provided to End Users.
		18.4.2 The Service Requirements for Document Copy and Print are listed below:
	2	**Print Services**
	3	Not applicable
	2	**Scanning Services**
	3	Not applicable
	2	**Facsimile Service**
	3	Not applicable
		18.5 Training
		18.5.1 Services to provide training to End Users in the use of ICT Services provided by the Supplier.
		18.5.2 The Service Requirements for Training are listed below:
	2	**General Requirements**

Requirement No.	Level	Requirement
	3	Not applicable
		18.6 Assistive Technology
		18.6.1 Provision of devices, Peripheral Equipment, and Software to support Assistive Technology End Users.
		18.6.2 The Service Requirements for Assistive Technology are listed below:
	2	**General requirements**
	3	Not applicable

Requirement No.	Level	Requirement
		19. TECHNICAL INFRASTRUCTURE SERVICES
		19.1 Environments
		19.1.1 The provision of a range of ICT Environments to support the testing and delivery of services to support FITS Services. Current services are provisioned with different levels of security administered and include:
		(a)
		(b)
		(c)
		(d) Access to selected End to End Services over the internet; and
		(e) Provision and management of environments to support testing.
		19.1.2 The Service Requirements for Environment Services are listed below:
	2	**Live Environments**
10-01-01-001-03	3	The Hosting Supplier shall provide, manage, maintain and support Hosting Services that are wholly or components of the Live Environments.
10-01-01-002-03	3	The Hosting Supplier shall provide, manage and maintain the components of the Hosting Services that form the Live Environments to ensure that they achieve the required Service Levels as defined in schedule 2.2 (Service Performance Management).
10-01-01-003-03	3	NOT USED

Requirement No.	Level	Requirement
10-01-01-003-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier, to ensure Live Environments for delivery of the FITS Services are Fully Functional.
10-01-01-003-11	3	The Hosting Supplier shall work and collaborate with the WAN and LAN Supplier, to ensure Live Environments for delivery of the FITS Services are Fully Functional.
10-01-01-005-03	3	The Hosting Supplier shall provide Hosting Services and management capabilities for Live Environments to securely segregate the Authority Hosted Applications at different Business Impact Levels in accordance with the Authority's ICT Information Assurance (IA) requirements as defined in schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan).
10-01-01-006-03	3	The Hosting Supplier shall provide Hosting Services and management capabilities to securely segregate internet facing Hosted Applications in accordance with the Authority's ICT Information Assurance (IA) requirements as defined in schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan).
10-01-01-007-03	3	The Hosting Supplier shall develop, implement, maintain and support a standard set of hosting components to be offered for use by Other Suppliers, as identified in the Dependencies Register, and Other Authority Providers, unless otherwise agreed.
10-01-01-008-02	3	The Hosting Supplier and Other Authority Providers shall work and collaborate with the EUCS Supplier to provide, maintain and support Live Environments to support the delivery of End to End Services including but not limited to: (i) Management Environments; and (ii) Operational Environments

Requirement No.	Level	Requirement
10-01-01-011-03	3	The Hosting Supplier shall ensure that the Hosting Services supplied in support of Live Environments utilise the most optimal efficient solution, while maintaining flexibility and scalability.
10-01-01-012-03	3	The Hosting Supplier shall, where required for the delivery of Live Environments, develop, implement, maintain and support Hosting Services including, but not limited to; (i) Co-location of FITS Suppliers, Third Parties and Other Authority Providers; (ii) Hosting of Authority Infrastructure and Applications; (iii) Traditional dedicated Hosting Services Environments; (iv) Shared Hosting Services Environments; (v) Multi-Tenanted Hosting Services Environments; (vi) Managed service provision of all components of the Hosting Services.
	2	**Non Live Environments**
10-01-02-001-03	3	The Hosting Supplier shall provide, manage, maintain and support Hosting Services that are wholly or components of the Non Live Environments.
10-01-02-002-03	3	The Hosting Supplier shall provide, manage and maintain the components of the Hosting Services that form the Non Live Environments to ensure that the Authority's Hosted Applications achieve the required Service Levels as defined in schedule 2.2 (Service Performance Management).
10-01-02-003-03	3	NOT USED
10-01-02-003-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier, to establish the Non Live Environments when required to support the delivery of FITS Services.

Requirement No.	Level	Requirement
10-01-02-005-03	3	
10-01-02-006-03	3	
10-01-02-007-03	3	
10-01-02-011-03	3	
10-01-02-013-03	3	
10-01-02-015-03	3	
10-01-02-016-03	3	The Hosting Supplier shall, where required for the delivery of Non Live Environments, develop, implement, maintain and support Hosting Services including, but not limited to; (i) Co-location of FITS Suppliers, Third Parties and Other Authority Providers; (ii) Hosting of Authority Infrastructure and Applications; (iii) Traditional dedicated Hosting Services Non Live Environments; (iv) Shared Hosting Services Non Live Environments; (v) Multi-Tenanted Hosting Services Non Live Environments; (vi) Managed service provision of all components of the Hosting Services.

Requirement No.	Level	Requirement
		19.2 Centralised Platform Services
		19.2.1 The provision of Hosting Services from an appropriate number of data-centres in alignment with Government ICT Strategy. The characteristics of Centralised Platform Services include, but will not be limited to;
		(a) Traditional data-centre hosting services;
		(b)
		(c)
		(d)
		(e)
		(f)
		(g)
		(h)
		19.2.2 Virtualisation and Shared Platform Services, includes, but is not limited to:
		(a) Virtualised ICT Environments with allocated resources which are independent from the underlying physical infrastructure; and
		(b) Shared ICT Environments where two or more components of the Hosting Service share resources.

Requirement No.	Level	Requirement
		19.2.3 Presentation Services are those with direct interaction with End Users.
		19.2.4 Web Hosting, Middleware and Database Services are the components of the multi-tier architectures typical of Hosting Services.
		19.2.5 Midrange and Mainframe Services encompass those Services that rely on specialist or proprietary hardware and operating systems.
		19.2.6 High Availability Services are typically those that are intolerant of outages during Service Hours and use hardware and/or Software within a single location or across two or more data-centres to mitigate against outages.
		19.2.7 The Service Requirements for Centralised Platform Services are listed below:
	2	**General Requirements**
10-02-01-001-03	3	The Hosting Supplier shall provide a set of Centralised Platform Services.
10-02-01-002-03	3	The Hosting Supplier shall publish the Centralised Platform Services in the FITS Service Catalogue in advance of provision of the Centralised Platform Service to the Hosting Supplier's ICT Environment unless otherwise agreed with the Authority.
10-02-01-003-03	3	Not used
10-02-01-004-03	3	The Hosting Supplier shall develop, implement, maintain, support Hosting Services comprised of dedicated infrastructure for the delivery of Hosting Services where the Authority has agreed that Shared Services or Multi-Tenanted services are not appropriate.

Requirement No.	Level	Requirement
10-02-01-005-03	3	The Hosting Supplier shall provide Hosting Services resources (either physical or virtual), that can be dynamically allocated to consumers of Hosting Services based on demand..
10-02-01-006-03	3	The Hosting Supplier shall be capable of pre-allocating Hosting Services resources in advance of demand, or where required by the Authority.
10-02-01-007-03	3	Not used
10-02-01-008-03	3	Not used
10-02-01-009-03	3	The Hosting Supplier shall implement, maintain and support Commercial Off The Shelf Software including the Operating Systems and infrastructure on which they run, to ensure that the Hosting Services can achieve the required Service Levels in accordance with schedule 2.2 (Service Performance Management).
10-02-01-010-03	3	The Hosting Supplier shall provide a Hosting Service that has characteristics that will include, but are not limited by, rapid on-demand provisioning and de-provisioning.
10-02-01-011-03	3	The Hosting Supplier shall work and collaborate with the Other Suppliers, as identified in the Dependencies Register, to establish the necessary Centralised Platform Services to support the delivery of FITS Services.
10-02-01-013-03	3	The Hosting Supplier shall work to reduce the number of server instances across the Hosting Service, where possible consolidating tasks from dedicated servers to Shared Hosting or Multi-Tenanted services.
	2	**Server Builds**
10-02-02-001-03	3	NOT USED
10-02-02-002-03	3	NOT USED
10-02-02-003-03	3	NOT USED

Requirement No.	Level	Requirement
10-02-02-004-03	3	The Hosting Supplier shall provide, manage and maintain a [minimal] common set of Server Builds used for the provision of the Hosting Service.
	2	**Virtualisation and Shared Platform Services**
10-02-03-001-03	3	The Hosting Supplier shall ensure, where the Hosting Supplier provides Virtualisation and Shared Platforms Services, that these services can securely segregate Application Software components and data at different Business Impact Levels in compliance with the relevant controls stated in the Security Controls (Objectives) Matrix.
10-02-03-002-03	3	Not used
10-02-03-003-03	3	Not used
	2	**Presentation Services**
	3	Not applicable
	2	**Middleware Services**
	3	Not applicable
	2	**Database Services**
	3	Not applicable
	2	**Web Hosting Services**
	3	Not applicable
	2	**Midrange Services**

Requirement No.	Level	Requirement
10-02-08-001-03	3	The Hosting Supplier shall provide, maintain and support Midrange Services for the delivery of Business Applications to Users.
10-02-08-002-03	3	The Hosting Supplier shall work to reduce the number of infrastructure and Platform components supporting the Midrange Services.
10-02-08-003-03	3	The Hosting Supplier shall provide the Authority with a report containing summary and detailed information on the reduction of the number of instances of Midrange Services across the Hosting Service every SRP, unless otherwise agreed with the Authority.
	2	**Mainframe Services**
10-02-09-001-03	3	Not used
	2	**High Availability Services**
10-02-10-001-03	3	The Hosting Supplier shall provide, maintain and support High Availability Services for the delivery of Business Applications to Users, to ensure unscheduled downtime to the service is minimised in the event of a failure of one or more of the Hosting Services components.
10-02-10-002-03	3	NOT USED
10-02-10-004-03	3	The Hosting Supplier shall develop, implement, maintain and support High Availability Services, to enable two or more server instances at a single Data Centre Facility to act as a single server instance for delivery of Hosting Services.
10-02-10-005-03	3	The Hosting Supplier shall develop, implement, maintain and support High Availability Services, to enable two or more server instances located across multiple Data Centre Facilities to act as a single server instance for delivery of Hosting Services.

Requirement No.	Level	Requirement
		19.3 Distributed Platform Services
		19.3.1 Distributed Platform Services is the provision of services to support infrastructure deployed into Local Server Rooms
		19.3.2 The Service Requirements for Hosting elements of Distributed Platform Services are listed below:
	2	**General Requirements**
	3	Not applicable
	2	**Server Builds**
	3	Not applicable
	2	**Virtualisation and Shared Platform Services**
	3	Not applicable
	2	**Presentation Services**
	3	Not applicable
	2	**Middleware Services**
	3	Not applicable
	2	**Database Services**
	3	Not applicable

Requirement No.	Level	Requirement
	2	**Web Hosting Services**
	3	Not applicable
	2	**Midrange Services**
	3	Not applicable
	2	**High Availability Services**
	3	Not applicable

Requirement No.	Level	Requirement
		19.4 Storage
		19.4.1 Storage refers to Devices used to retain and retrieve data; examples include, but are not limited to;
		(a) Storage Area Networks;
		(b) Network Attached Storage;
		(c) Directly attached disc; and
		(d) Tape libraries.
		19.4.2 The Storage Devices shall provide the capability of servicing the different performance and cost requirements of the Hosted Services including, but not limited to:
		(a) File Stores; and
		(b) Databases.
		19.4.3 The Hosting supplier shall provide Storage with the capability to automatically move data to lower cost Storage in a manner that is transparent and without interruption to the FITS Service that rely on the Storage. Examples may include, but are not limited to:
		(a) Hierarchal Storage Management; and
		(b) Tiered Storage.
		19.4.4 The Service Requirements for Storage Services are listed below:

Requirement No.	Level	Requirement
	2	**General Requirements**
10-04-01-001-03	3	The Hosting Supplier shall provide, maintain and support Storage systems for the delivery of Business Applications; including, but not limited to: Storage Area Networks, Network Attached Storage, Local Disk sub-systems.
10-04-01-002-03	3	The Hosting supplier shall offer Storage services that include, but are not limited to the following characteristics; (i) Storage virtualisation (ii) Multi-tiered Storage systems comprised of 3+ tiers of Storage each with different performance and cost characteristics; (iii) Automatic redistribution of data to different tiers in a way invisible to the dependent Operating Systems and Business Applications; (iv) Data portability to enable data to be moved easily and simply from one Storage System to another; (v) Backup and Archive capabilities.
	2	**Unstructured Data Services / File Store**
10-04-02-001-03	3	The Hosting Supplier shall provide, maintain and support Unstructured Data Services / File Store for the delivery of Business Applications in compliance with the Authority's Information Lifecycle Management Policy.
10-04-02-003-03	3	Not used
10-04-02-006-03	3	Not used

Requirement No.	Level	Requirement
	2	**Structured Data Services**
10-04-03-001-03	3	The Hosting Supplier shall provide, maintain and support Structured Data Services for the delivery of Business Applications.
10-04-03-002-03	3	Not used
10-04-03-005-03	3	The Hosting Supplier shall provide, maintain and support an automatic system to move data within Structured Data Services to different tiers of Storage in compliance with the Authority's Information Lifecycle Management Policies and the SIAM Supplier's Information Lifecycle Management Processes and Procedures.
		19.5 Bulk Print
		19.5.1 The services that support the fulfilment of large volume print jobs.
		19.5.2 The Service Requirements for Bulk Print are listed below:
	2	**General requirements**
	3	Not applicable

Requirement No.	Level	Requirement
		19.6 Backup and Recovery Services
		19.6.1 The provision of systems for retention and retrieval of data without loss of fidelity, if for any reason the original of the data becomes unavailable.
		19.6.2 The Service Requirements for Backup and Recovery Services are listed below:.
	2	**General requirements**
10-06-01-001-03	3	The Hosting Supplier shall comply with the Authority's Backup and Recovery Policy.
10-06-01-003-05	3	The Hosting Supplier shall produce Backup and Recovery Policies, Processes and Procedures for Business Applications not less than Thirty (30) Working Days before Service Commencement Date for Approval by the Authority.
10-06-01-004-03	3	The Hosting Supplier shall provide, maintain and support Backup and Recovery Services in support of the delivery of Hosting Services and Business Applications.
10-06-01-005-03	3	The Hosting Supplier shall document details of the Backup and Recovery Service Policies, Processes and Procedures for Hosting Services for Approval within three (3) Months of the Effective Date.
10-06-01-006-03	3	The Hosting Supplier's Backup and Recovery Service Policies, Processes and Procedures for Hosting Services shall be updated and Approved prior to all Service Commencement Dates.

Requirement No.	Level	Requirement
10-06-01-007-03	3	The Hosting Supplier shall securely backup, retain and restore Business Applications in the Hosting Supplier ICT Environments in accordance with the Authority's Archive Policy and the Authority's Record Retention Schedules. This will include but will not be limited to :- (i) Live Data (ii) Archive Data (iii) Test Data (iv) Operating Systems; (v) Business Application and system configurations; (vi) Business Application related Data, files and documents; (vii) Logs and Audit trails.
10-06-01-009-03	3	The Hosting Supplier shall provide a Backup and Recovery Service report each SRP to the SIAM supplier: (i) Confirming that all Authority Data has been successfully backed up and retained in accordance with the Hosting Supplier's Backup and Recovery Service Policies, Processes and Procedures (ii) Describing any instances where backups of Authority Data has not been successful (iii) Proposing a Recovery Plan to mitigate future failures in meeting Backup and Recovery Service Policies, Processes and Procedures.
10-06-01-011-03	3	The Hosting Supplier shall provide Backup and Recovery Service that complies with the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the Business Applications or associated Data.

Requirement No.	Level	Requirement
10-06-01-012-03	3	The Hosting Supplier shall, on an Annual basis, demonstrate to the Authority the Hosting Supplier's ability to fully restore Business Applications and Data in accordance with the Hosting Supplier's Backup and Recovery Service Policies, Processes and Procedures and meet both the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO).
10-06-01-013-03	3	The Hosting Supplier shall ensure any Data backups and Archive Data that will be sent to, from or between Hosting Supplier's Sites shall be transferred in accordance with the Authority's Data Handling Policies as set out in schedule 2.3 (Standards), unless otherwise agreed by the Authority.
10-06-01-014-03	3	The Hosting Supplier shall provide secure storage for any removable storage media, in accordance with the Authority's Security Policies, Processes and Procedures as set out in schedule 2.5 (Security Management Plan).
	2	**Self Service Data Retrieval**

Requirement No.	Level	Requirement
	3	Not applicable
		19.7 Archive Services
		19.7.1 The provision of automatic systems for retention, retrieval and disposal of digital data in accord with the Authority Information Lifecycle Management (ILM) Policy. This service is distinct from the Backup and Recovery Services which may or may not be relevant within an overall strategy of availability.
		19.7.2 Mechanisms to archive, recover and delete material should be a combination of automatic (for example, automatic archive based on defined rules) and self service (i.e. at End User instigation) so minimising the needs of End Users to contact the service desk.
		19.7.3 The benefit of this service to the Authority is as follows:
		(a) Provides for, automatic retention, recovery and deletion of digital data from the Storage, according to the ILM Policy; and
		(b) Potential for cost effective Storage of archive material through the automatic use of Storage hierarchies of decreasing cost.
		19.7.4 The Service Requirements for Archive Services are listed below:
	2	**General requirements**
10-07-01-001-03	3	The Hosting Supplier shall provide an Archive Service that complies with the Authority's Archive Policy and the Authority's Record Retention Schedules.
	2	**File Archiving Service**

Requirement No.	Level	Requirement
	3	Not applicable
		19.8 Data Management
		19.8.1 The provision of service for enforcement of the Information Lifecycle Management Policy, including, but not limited to, creation and management of master data, meta-data, schema and any other types of associated data.
		19.8.2 The Service Requirements for Data Management are listed below:
	2	**Information Lifecycle Management**
10-08-01-001-03	3	The Hosting Supplier shall manage the Data within the Business Applications in accordance with the Authority's Information Lifecycle Management Policy and the SIAM Suppliers' Information Lifecycle Processes and Procedures.
10-08-01-002-03	3	The Hosting Supplier shall support the SIAM Supplier in the creation and maintenance of the Information Lifecycle Management Processes and Procedures.
10-08-01-003-03	3	The Hosting Supplier will work and collaborate with the AMS Supplier in the provision of Information Lifecycle Management services to archive Business Application data in accordance with the Authority's Information Lifecycle Management Policy and the SIAM Suppliers' Information Lifecycle Processes and Procedures.

Requirement No.	Level	Requirement
		19.9 Software Readiness Service
		19.9.1 The preparation of Software, Applications, components (or a combination of any or all of these), in readiness for provisioning to Devices. Examples of this would be packaging / wrapping / or sequencing of Software in order to remotely install or stream Applications to servers.
		19.9.2 The Service Requirements for Software Readiness Services are listed below:
	2	**General requirements**
10-09-01-001-03	3	The Hosting Supplier shall provide and maintain a Software Readiness Service that shall deliver a standard, consistent mechanism for preparing and testing Software in readiness for provisioning into the Hosting Supplier's ICT Environment.
10-09-01-002-03	3	The Hosting Supplier shall develop the Hosting Service Software Readiness Policies, Processes and Procedures for provisioning Business Applications into the Hosting Supplier's ICT Environment, attain Approval from the Authority and publish them to the SKMS within three (3) Months of the Effective Date.
10-09-01-003-03	3	The Hosting Supplier shall update the Hosting Service Software Readiness Policy, Processes and Procedures not less than annually following the Effective Date and make the updated documents available to Suppliers through the SKMS within one (1) day of the update being Approved.
10-09-01-004-03	3	The Hosting Supplier shall comply with the Hosting Service Software Readiness Policies, Processes and Procedures for provisioning Business Applications into the Hosting Supplier's ICT Environment, unless otherwise agreed with the Authority.
10-09-01-006-03	3	The Hosting Supplier shall provide a Software Readiness Service for Software which has been provided by Suppliers and Other Authority Providers to be deployed onto the Hosting Supplier's ICT Environment.

Requirement No.	Level	Requirement
		19.10 Local Server Rooms
		19.10.1 Local Server Rooms provides and maintains the infrastructure around local and distributed data rooms and communications rooms and will be managed by the EUCS Supplier.
		19.10.2 The Service Requirements for Local Server Rooms are listed below:
	2	**General requirements**
	3	Not applicable

Requirement No.	Level	Requirement
		19.11 Data Centre Facilities Service
		19.11.1 The provision, maintenance and support of physical environments with the appropriate power, cooling, security and technical capability with the capability to deliver the Services required by the Authority.
		19.11.2 The Data Centre Facilities Service includes the physical Data Centre space that shall be provided by the Data Centre Supplier, which will offer amenities that include but are not limited to:
		(a) Separation of the facilities, such that the risk of concurrent loss of both facilities is very low; loss includes, but is not limited to natural or man-made disaster;
		(b) Capability to allow Synchronous replication between the facilities;
		(c) Green credentials - Compliance with the latest version of the EU Code of Conduct on Data Centres Energy Efficiency to help attain the Greening Government ICT Strategy;
		(d)
		(e)
		19.11.3 The Data Centre Supplier shall provide the Data Centre Facilities Service for use by the Hosting Supplier and Other Suppliers.
		19.11.4 The Service Requirements for Data Centre Facilities Service are listed below:
	2	**General requirements**

Requirement No.	Level	Requirement
10-11-01-001-03	3	The Hosting Supplier shall ensure technology, Applications, system, Data and service architectures and designs minimise, de-duplicate and rationalise the use of Hosting Supplier equipment and the power required to operate it.
10-11-01-017-10	3	The Hosting Supplier shall use the Data Centre Facilities provided to them by the Data Centre Supplier.
10-11-01-024-10	3	The Hosting Supplier shall provide their requirements for hosting of non-rack mounted equipment, to the Data Centre Supplier within ten (10) Working Days of the Effective Date.
10-11-01-026-10	3	The Hosting Supplier making use of the Data Centre Supplier's Data Centre Facilities shall ensure that any Devices installed into the Data Centre Facilities are connected to both the diverse power feeds provided by the Data Centre Supplier, in accordance with the Data Centre Supplier's Data Centre Facilities Service Standards, Policies, Processes and Procedures.
10-11-01-028-10	3	The Hosting Supplier shall request the Data Centre Supplier's Data Centre Facility Services from the FITS Service Catalogue unless otherwise agreed by the Authority.
10-11-01-031-10	3	The Hosting Supplier making use of the Data Centre Facilities shall comply with the Data Centre Supplier's Data Centre Facilities Service Standards, Policies, Processes and Procedures.
10-11-01-035-10	3	The Hosting Supplier shall accept deliveries and use the secure storage areas (of a size no less than three (3) metres wide, three (3) metres deep and two and a half (2.5) metres high) provided to them by the Data Centre Supplier for the storage of ICT equipment.
10-11-01-037-10	3	The Hosting Supplier shall use the equipment build and test areas (of a size no less than five (5) metres wide, four (4) metres deep and two and a half (2.5) metres high) provided to them by the Data Centre Supplier for the building and testing of ICT equipment.
10-11-01-038-10	3	The Hosting Supplier shall fit out, maintain and support the equipment build and test area provided by the Data Centre Supplier for each Data Centre Facility.

Requirement No.	Level	Requirement
10-11-01-040-10	3	The Hosting Supplier shall use the office facilities (which includes a room of a size no less than four (4) metres wide, four (4) metres deep and two and a half (2.5) metres high) provided to them by the Data Centre Supplier for their onsite support personnel.
10-11-01-041-10	3	The Hosting Supplier shall fit out, maintain and support the office facilities provided by the Data Centre Supplier.
10-11-01-044-10	3	The Hosting Supplier shall make use of the common facilities provided by the Data Centre Supplier. These common facilities shall at a minimum shall consist of the following:- cleaning, toilets, showers, kitchen, first aid, car parking and rest areas.
10-11-01-048-10	3	The Hosting Supplier shall ensure personnel attend the Data Centre Supplier's training courses prior to their commencement of work at the Data Centre Facility.

Requirement No.	Level	Requirement
		19.12 Directory Services
		19.12.1 The Directory Service within EUCS provides integrated directory services for all FITS Services which require them in accordance with the FITS Directory Services Architecture View and Identity and Directory Architecture standards.
		19.12.2 The benefits of this service to the Authority are as follows:
		(a) A single efficient, fit for purpose Directory Service for the Authority;
		(b) Enables such facilities as consolidated contacts directories for messaging and calendaring; and
		(c) Provides a centralised, consistent view of identity for authentication, authorisation, accounting and audit purposes.
		19.12.3 The Service Requirements for Directory Services are listed below:
	2	**General Requirements**
10-12-01-001-03	3	The Hosting Supplier shall provide, maintain and support Infrastructure Directory Services for the delivery of Hosting Services.
10-12-01-002-03	3	NOT USED
10-12-01-006-03	3	The Hosting Supplier shall design, provide, maintain and support one or more Application Directories to sustain all Authentication and Authorisation to and by Application entities within the Directory Service, in accordance with the Authority's Access Management Policy and the SIAM Supplier's Access Management Processes and Procedures.

Requirement No.	Level	Requirement
10-12-01-008-03	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier to ensure that the Hosting Services Application Directories are integrated with Directory Services or synchronised with Identity and Access Management as agreed with the Authority.
10-12-01-012-02	3	The Hosting Supplier and Other Authority Providers may request via the FITS Service Catalogue that the EUCS Supplier makes available to them the Directory Services either for existing Services or in order to commission additional Services that will rely on the Directory Services.
10-12-01-027-02	3	The Hosting Supplier and Other Authority Providers shall work and collaborate with the EUCS Supplier to define the delegated privileges and access to Infrastructure Directories provided by the EUCS Supplier required to support the delivery of FITS Services.
10-12-01-028-02	3	The Hosting Supplier and Other Authority Providers shall work and collaborate with the EUCS Supplier to define identity attributes for inclusion in Master or Infrastructure Directories to support the delivery of FITS Services.
10-12-01-032-02	3	The Hosting Supplier shall comply with the EUCS Supplier's Directory Services Policies, Processes and Procedures in the provision or integration of Directory Services.
10-12-01-034-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier if they require the use of the EUCS Supplier's single sign on capability to support the Hosting Services where they authenticate against the EUCS Infrastructure Directory.
10-12-01-035-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier if they require the use of the EUCS Supplier's single sign on capability to support their Services.

Requirement No.	Level	Requirement
		19.13 Identity and Access Management
		19.13.1 Identity and Access Management provides the Identity management, and consequent Authentication and Authorisation (A&A) for all EUCS Services. It relies on the Directory Service as a source of that Identity information.
		19.13.2 The 'FITS Identity and Access Management View' document describes the IdAM architecture and approach which the Authority expects the FITS Suppliers to adopt. The benefit of this service to the Authority is a single, effective, secure and authoritative approach to identity and access control.
		19.13.3 The Service Requirements for Identity and Access Management Services are listed below:
	2	**General requirements**
10-13-01-001-03 (Common)	3	The Hosting Supplier shall implement and enforce the Authority's Password Management Policy for the Hosting Services, unless otherwise agreed with the Authority.
10-13-01-004-02	3	Not Used
10-13-01-022-02	3	Not Used
10-13-01-024-02	3	Not Used
10-13-01-033-02	3	The Hosting Supplier and Other Authority Providers shall work and collaborate with the EUCS Supplier where they require the use of the EUCS Supplier's Identity and Access Management Service to support the Authority's Access Management Policy and the SIAM Supplier's User Administration Policy.

Requirement No.	Level	Requirement
10-13-01-041-02	3	The Hosting Supplier shall comply with the EUCS Supplier's Identity and Access Management Service Processes and Procedures in delivering the Hosting Services which utilise the EUCS Supplier's Identity and Access Management Service.
10-13-01-049-02	3	
10-13-01-052-02	3	
10-13-01-053-02	3	
10-13-01-057-02	3	
10-13-01-060-02	3	
10-13-01-082-02	3	

Requirement No.	Level	Requirement
		19.14 Public Key Infrastructure
		19.14.1 The Network Supplier shall provide, maintain and support a PSN compliant Public Key Infrastructure (PKI) and Encryption Management Service that supports the secure communication and internetworking between Devices at the appropriate Business Impact Level in the provision of FITS Services.
		19.14.2 The PKI Service will be established in line with PSN Standards and provided under the PSN framework. The document 'FITS – PKI Architecture' describes the Authorities expectation for PKI. The PKI Service will be implemented and managed in accordance with that document.
		19.14.3 The PKI Service will be available as a service to other FITS Suppliers which require it, including FITS Services delivered by the Suppliers and Other Authority Providers.
		19.14.4 The benefits of the Public Key Infrastructure Service to the Authority include the following:
		(a) A single, managed and PSN compliant PKI Service used for encryption and identity validation in the provision of FITS Services.
		(b) The IA benefits associated with a well architected and delivered PKI.
		19.14.5 The Service Requirements for PKI Services are listed below:
	2	**General requirements**
10-14-01-005-04	3	The Hosting Supplier shall utilise the Network Supplier's PKI Service unless otherwise agreed with the Authority

Requirement No.	Level	Requirement
10-14-01-006-04	3	The Hosting Supplier shall provide, maintain and support PKI services to support the delivery of Hosting Services. The Hosting Supplier's PKI service shall be subordinate to the Network Supplier's PKI service unless otherwise agreed with the Authority.
10-14-01-009-04	3	The Hosting Supplier's PKI services shall be delivered in accordance with the Authority's PKI Policy and PSN Policies referenced within schedule 2.3 (Standards).
		19.15 Internet Access Service
		19.15.1 Internet access is the provision of public internet services (moderated and audited in accordance with the Authorities internet access policies) to the ICT Environment.
		19.15.2 The Service Requirements for Internet Access Service are listed below:
	2	**General requirements**

Requirement No.	Level	Requirement
	3	Not applicable
		20. NETWORK INFRASTRUCTURE SERVICES
		20.1 Core Network Services
		20.1.1 Core Network Services provides a number of key network services for all FITS services:
		(a) IP Address Management: the process and technology involved in defining IP schemas, allocating IP addresses to devices on a dynamic / reserved / fixed basis (e.g. through the implementation of Dynamic Host Configuration Protocol services), and ensuring that unused addresses are available to be used by other Devices;
		(b) Master Time Reference: often required for transaction/replication services, time services provide access to a trusted time source to synchronise the various components of the FITS Services;
		(c) Domain Name Service (DNS): translates queries for domain names into IP addresses for the purpose of locating computer services and devices; and
		(d) Network Optimization: provides a number of sub-services (including traffic marking) which allows the business to prioritise network traffic to fulfil business need e.g. Quality of Service (QoS).
		20.1.2 The Service Requirements for Core Network Services are listed below:
	2	**IP Address Management**
11-01-01-001-03 (Common)	3	The Hosting Supplier shall deliver the Hosting Services in accordance with the Authority's IP addressing Policy.
11-01-01-013-04	3	NOT USED

Requirement No.	Level	Requirement
11-01-01-015-04	3	The Hosting Supplier shall manage the allocation of IP addresses to deliver their Services.
11-01-01-019-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier to provide any Device configuration information that is required to be applied by the Dynamic IP Address Allocation Service.
11-01-01-021-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier to ensure that the dynamic IP address allocation Service can register their Devices with the Domain Name Service.
	2	**Master Time Reference**
11-01-02-001-03	3	The Hosting Supplier shall ensure that all components used in the delivery of Hosting Service have their time synchronised with a Master Time Reference.
11-01-02-002-03	3	The Hosting Supplier shall ensure that devices used in the delivery of Hosting Services are within one (1) second of the Master Time Reference.
11-01-02-003-04	3	The Hosting Supplier shall use the Master Time Reference in the delivery of the Hosting Services as supplied by the Network Supplier or use a stratum zero time source.
	2	**Domain Naming Service**
11-01-03-001-03	3	The Hosting Supplier shall provide, maintain and support an internal DNS Service for use within the Hosting Supplier ICT Environment. This shall include the management of the DNS namespace and the structure of the domains that comprises the internal domain name.
11-01-03-002-03	3	The Hosting Supplier shall work and collaborate with Other Suppliers, as identified in the Dependencies Register, and Other Authority Providers in the support and maintenance of the Hosting Suppliers Domain Naming Service
11-01-03-003-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to ensure that the external and Hosting internal DNS Services are integrated to provide DNS resolution for the delivery of FITS Services to the required Service Levels.

Requirement No.	Level	Requirement
11-01-03-005-03	3	The Hosting Supplier shall be responsible for registering any external namespaces required to support the Hosting Services, with the relevant PSN or public internet providers.
11-01-03-006-04	3	The Hosting Supplier shall be responsible for registering any external namespaces required to support the Hosting Services, with the Network Supplier or relevant public domain registrars.
11-01-03-006-03	3	The Hosting Supplier shall make available the Hosting internal DNS Service to Other Suppliers as identified in the Dependencies Register to be used within the Hosting Supplier ICT Environment.
11-01-03-012-02	3	The Hosting Supplier, shall be responsible for registering with the EUCS Supplier, any internal DNS records required to present Hosting Services to the FITS Supplier ICT Environment.
11-01-03-017-02	3	The Hosting Supplier shall work and collaborate with the EUCS Supplier where required, to ensure that internal DNS Services provide Fully Functional DNS resolution for the provision of FITS Services.
	2	**Network Performance Optimisation**
11-01-04-002-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to host Network Performance Optimisation Devices or technologies, where appropriate in the Hosting Supplier's ICT Environments to support the delivery of FITS Services.
11-01-04-002-11	3	The Hosting Supplier shall work and collaborate with the WAN and LAN Supplier to host Network Performance Optimisation Devices or technologies, where appropriate in the Other FITS Supplier's ICT Environments to support the delivery of FITS Services
11-01-04-005-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to ensure that where Network Performance Optimisation technologies are deployed, all elements operate efficiently and effectively to support the delivery of FITS Services.
11-01-04-005-11	3	

Requirement No.	Level	Requirement
11-01-04-007-04	3	
11-01-04-007-11	3	
11-01-04-009-04	3	
11-01-04-011-11	3	
11-01-04-012-04	3	
11-01-04-014-04	3	
	2	**Encryption Services**
	3	Not applicable

Requirement No.	Level	Requirement
		20.2 LAN
		20.2.1 The ability to provide and manage LAN services and within its scope is all connectivity, including physical cables, from WAN points through to Devices on the network. The scope of LAN Services includes routers, switches and wireless Devices (where provided) together with configuration and management, support and Documentation.
		20.2.2 The benefit of this service to the Authority is a single, effective, centralised point of contact to support all LAN services within the Hosting Service.
		20.2.3 The Service Requirements for LAN Services are listed below:
	2	**LAN Services**
11-02-01-001-03	3	The Hosting Supplier shall develop, implement, maintain and support LAN Services in the Hosting Services ICT Environments.
11-02-01-002-03	3	The Hosting Supplier shall ensure that the LAN Services are compliant with the PSN Standards for QoS prior to connecting them to the network, unless otherwise agreed.
	2	**LAN Port Services**
	2	**Wireless LAN Services**
	3	Not applicable

Requirement No.	Level	Requirement
		20.3 WAN
		20.3.1 The ability to provide and manage WAN services and within its scope is all connectivity, including physical cables, devices and any associated software, logic or services together with configuration and management, support and documentation.
		20.3.2 The majority of WAN Services will be provided by the Network Supplier; exceptions to this are WAN services solely provided to support the Hosting Service, examples include, but are not limited to;
		(a) Internet Connectivity for Business Applications that need to be presented over the internet; and
		(b) Inter-data-centre connectivity between Hosting Service facilities.
		20.3.3 The benefit to the Authority is a single, effective, centralised point of contact to support all WAN services within the Hosting Service.
		20.3.4 The Service Requirements for WAN Services are listed below:
	2	**WAN Services**
11-03-01-002-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to facilitate the connection of the WAN to their LAN to support the delivery of the FITS Services.
11-03-01-002-11	3	The Hosting Supplier shall work and collaborate with the WAN and LAN Supplier to facilitate the connection of the WAN provided by the WAN and LAN Supplier to the [TOWER] Supplier LAN to support the delivery of the FITS Services.
	2	**Broadband Services**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Internet Connectivity Service**
11-03-03-003-04	3	NOT USED
11-03-03-003-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to implement Gateway Services and the required security controls for the Internet Connectivity Service in accordance with the Authority's ICT IA Policies, Processes and Procedures.
11-03-03-005-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to ensure that, where Hosting Services are using the Internet Connectivity Service, they are Fully Functional and meet the Service Levels as set out in the schedule 2.2 (Service Performance Management).
	2	**Cross Site Connectivity**
11-03-04-002-10	3	The Hosting Supplier shall make use of the dense wave division multiplexing (DWDM) Cross Site Connectivity Service, provided by the Data Centre Supplier, for transfer of data between the Data Centre Supplier's Data Centre Facilities.
11-03-04-003-10	3	The Hosting Supplier shall provide the management, monitoring and reporting of services they provide that use the dark fibre or equivalent connectivity, provided by the Data Centre Supplier, between the Data Centre Facilities for cross site connectivity.
11-03-04-004-10	3	
11-03-04-008-10	3	
	2	**Voice over IP**
	3	Not applicable

Requirement No.	Level	Requirement
	2	**Satellite**
	3	Not applicable
		20.4 Telephony
		20.4.1 Telephony provides the full range of Telephony Services required by the Authority:
		(a) Hardware and Software including telecommunications switches, operator consoles and audio conferencing;
		(b) Functionality to allow the Authority to make and receive calls (including voicemail, call management and audio conferencing);
		(c) Access to services via the PSN or PSTN;
		(d) Provision of digital and analogue telephony;
		(e) Provision of services in support of IL4 accreditation for high security Telephony; and
		(f) Provision of Telephony Services to include Interactive Voice Response to Authority contact centres.
		20.4.2 The Service Requirements for Telephony are listed below:
	2	**Telephony Core Infrastructure**
	3	Not applicable
	2	**Analogue Telephony Services**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Mobile Network**
	3	Not applicable
	2	**Contact Centre Services**
	3	Not applicable
		20.5 Video Services
		20.5.1 The provision of Video Services, both at an enterprise scale and specific video capabilities supporting the delivery of justice such as in court / prison video services.
		20.5.2 The Service Requirements for Video Services are listed below:
	2	**In Court / Prison Video Services**
	3	Not applicable
	2	**Enterprise Video Services**
	3	Not applicable

Requirement No.	Level	Requirement
		20.6 Remote Access Services
		20.6.1 Remote Access Services enable End Users to access End to End Services.
		20.6.2 The Service Requirements for Remote Access Services are listed below:
	2	**Secure Remote Access**
	3	Not applicable
	2	**Untrusted Remote Access**
	3	Not applicable

Requirement No.	Level	Requirement
		20.7 Gateway Services
		20.7.1 Gateways provide a point of demarcation between two or more different ICT Environments where security controls are implemented. Examples include Gateways between:
		(a) Different Supplier or Service boundaries within the FITS ICT Supplier Environments - defined as Boundary Gateways.
		(b) Different Accreditation boundaries, at the same impact level - where the risk profile and/or accreditation scope on either side is different. These are defined as Inter-Operability Gateways.
		(c) Different Impact Levels or Protective Markings – i.e. between ICT Environments in different risk domains. These are defined as Inter-Domain Gateways.
		20.7.2 The 'FITS – Access Gateway Architecture View' describes the Authorities expectation for Gateway Services. The Gateway Services will be established in line with the relevant IA Polices Processes and Procedures and CESG standards.
		20.7.3 The security controls deployed within each type of Gateway may consist of:
		(a) Common security controls - which may protect a number of different services.
		(b) Service-specific controls – which may protect a particular service. Examples include content scanners for email or session border controllers for IP based voice and video services.
		20.7.4 The Network Supplier will provide maintain and support
		(a) All Gateway Services required for delivery of their own services.

Requirement No.	Level	Requirement
		(b) Gateway Services providing common security controls required for the delivery of FITS Services by the Suppliers. This will be located within the Data Centre Facilities provided by the Data Centre Supplier, and Authority Sites as required.
		(c) The facility for the Suppliers and Other Authority Providers to provide and integrate additional service-specific security controls with the Gateway Services.
		(d) Gateway Services to enable the integration of the FITS ICT Environment with ICT Environments provided by Other Authority Providers.
		(e) Gateway Services for use by the Suppliers and Other Authority Providers to gain management access to FITS Services – both within the Data Centre Facilities provided by the Data Centre Supplier, and Authority Sites as required.
		20.7.5 The Other Suppliers will:
		(a) Provide maintain and support any service-specific security controls required in the provision of their services and integrate these with the Gateway Services provided by the Network Supplier.
		(b) Utilise the Gateway Services provide by the Network Supplier to gain management access to FITS Services - both within the Data Centre Facilities provided by the Data Centre Supplier, and Authority Sites as required.
		20.7.6 The benefits of Gateway Services to the Authority include the following:
		(a) Enables secure data flow and service access between different ICT Environments.
		(b) Consistent application of security controls between ICT Environments in line with the Authority's policy processes and procedures.

Requirement No.	Level	Requirement
		20.7.7 The Service Requirements for Gateway Services are listed below:
	2	**General Requirements**
11-07-01-004-04	3	The Hosting Supplier shall, when providing services within the Data Centre Facilities provided by the Data Centre Supplier, or at Authority Sites, use the Gateway Services provided by the Network Supplier to provide common security controls required for the delivery of FITS Services.
11-07-01-008-04	3	The Hosting Supplier shall integrate, provide, maintain and support security controls specific to the Hosting Services within the Gateway Services provided by the Network Supplier, in accordance with the Authority's IA Policies Processes and Procedures.
	2	**Boundary Gateways**
	3	Not applicable
	2	**Interoperability Gateways**
11-07-03-002-04	3	The Hosting Supplier shall integrate, provide, maintain and support security controls specific to the Hosting Services within the Interoperability Gateways provided by the Network Supplier, in accordance with the Authority's IA Policies Processes and Procedures.
	2	**Inter-Domain Gateways**
11-07-04-002-04	3	The Hosting Supplier shall integrate, provide, maintain and support security controls specific to the Hosting Services within the Inter-Domain Gateways provided by the Network Supplier, in accordance with the Authority's IA Policies Processes and Procedures.

Requirement No.	Level	Requirement
	2	**Management Gateway Service**
11-07-05-003-04	3	The Hosting Supplier and Other Authority Providers shall use the remote access service provided by the Network Supplier to access the Management ICT Environments within the Data Centre Facilities provided by the Data Centre Supplier, and Authority Sites, to enable support of FITS Services from Supplier's Sites, unless otherwise agreed with the Authority.
11-07-05-004-04	3	The Hosting Supplier shall provide maintain and support the security controls required to control management access to the Hosting services hosted within the Data Centre Facilities provided by the Data Centre Supplier and Authority Sites, including but not limited to: (i) Presentation Services (i) Bastion Host System Devices; (ii) Authentication and Authorisation of Supplier Personnel access; (iii) Presentation of systems management tooling. These controls shall be provided in accordance with the Authority's IA Policies, Processes and Procedures and the Authority's Access Management Policy
11-07-05-009-04	3	The Hosting Suppliers shall enable controlled access to the Hosting Supplier’s ICT Environments to Other Suppliers and Other Authority Providers as requested for the purposes of supporting FITS Services.

Requirement No.	Level	Requirement
		20.8 Network Integration Services
		20.8.1 This is the support that the Hosting Supplier will provide to the Network Supplier in the technical integration of Network Services with Hosting Services
		20.8.2 The Service Requirements for Network Integration Services are listed below:
	2	**General Requirements**
	2	**WAN and LAN Supplier Management**
	3	Not Applicable
	2	**Network Interconnect Services**
11-08-03-003-04	3	The Hosting Supplier shall work and collaborate with the Network Supplier to ensure that where Hosting Services are using the Network Interconnect Service they are Fully Functional and meet the Service Levels as set out in schedule 2.2 (Service Performance Management).

Requirement No.	Level	Requirement
		21. APPLICATION SERVICES
		21.1 Application Design and Development
		21.1.1 The design and development of new Business Applications, including the analysis of requirements, design, development, and provision of PRISM.
		21.1.2 The Service Requirements for Application Design and Development are listed below:
	2	**General Requirements**
	3	Not applicable
	2	**Analysis of Application Requirements**
	3	Not applicable
	2	**High Level Design**
	3	Not applicable
	2	**Detailed Design**
	3	Not applicable
	2	**PRISM (Post Release Implementation Support and Maintenance)**
	3	Not applicable

Requirement No.	Level	Requirement
	2	**Proof of Concept Service**
	3	Not applicable
		21.2 Application and Database Management
		21.2.1 The process by which application data is acquired, validated, stored, protected, and processed, and by which its accessibility, reliability, and timeliness is ensured to satisfy the needs of the data user.
		21.2.2 The Service Requirements for Application and Database Management are listed below:
	2	**General requirements**
	3	Not applicable
	2	**Application Data Management**
	3	Not applicable
		21.3 Application Enhancements
		21.3.1 Application development services for enhancements to existing Business Applications.
		21.3.2 The Service Requirements for Application Enhancements are listed below:
	2	**General requirements**
	3	Not applicable

Requirement No.	Level	Requirement
		21.4 Application Integration
		21.4.1 Integration of applications with other services.
		21.4.2 The Service Requirements for Application Integration are listed below:
	2	**Short Messaging Service**
	3	Not applicable
		21.5 Collaboration Toolset
		21.5.1 This provides a number of collaboration services to Users.
		21.5.2 The Service Requirements for Collaboration Toolset are listed below:
	2	**Messaging Services**
	3	Not applicable
	2	**Calendar Services**
	3	Not applicable
	2	**Address Book Services**
	3	Not applicable
	2	**Office Automation**

Requirement No.	Level	Requirement
	3	Not applicable
	2	**Presence and Instant Messaging**
	3	Not applicable
	2	**Workgroup Collaboration and Sharing**
	3	Not applicable
	2	**Device and Enterprise Search**
	3	Not applicable

Requirement No.	Level	Requirement
		22. PROJECT DELIVERY MANAGEMENT
		22.1 Project Management
		22.1.1 Project Management is a critical activity within Project Delivery Management and aims to ensure appropriate Project Management skills and resources are available as and when required by the Authority.
		22.1.2 The Project Management requirements describe the responsibilities of the Hosting Supplier with regards to a consistent approach to, and governance of, all stages of a project's lifecycle in accordance with industry leading methodologies as defined in the Policies, Processes and Procedures set down by the Authority.
		22.1.3 The main objectives for Project Management are to:
		(a) Provide the Authority with an accessible mechanism to supplement existing skills and resources on an ad hoc basis to address the variable needs of the business;
		(b) Ensure a consistent approach to project management is adopted by all Suppliers to drive a more integrated governance and delivery capability;
		(c) Assure compliance to the Authorities Policies, Processes and Procedures; and
		(d) Ensure a consistent approach to the delivery of new FITS Services.
		22.1.4 The General Requirements for Project Management are listed below:
	2	**General requirements**

Requirement No.	Level	Requirement
13-01-01-001-03 (Common)	3	The Hosting Supplier shall provide and maintain a Project Management service which is aligned to the Authority's Project Management Policies, Processes and Procedures.
13-01-01-002-03 (Common)	3	The Hosting Supplier shall at all times, comply with the Authority's Project Management Policies, Processes and Procedures.
13-01-01-003-03 (Common)	3	The Hosting Supplier shall work and collaborate with Other Suppliers, Other Authority Providers and the Authority, as identified in the Dependencies Register, to deliver Project Management services in compliance with the Authority's Project Management Policies, Processes and Procedures
13-01-01-004-03 (Common)	3	The Hosting Supplier shall work and collaborate with the Authority in any review as a result of the Hosting Supplier's non compliance with the Authority's Project Management Policies, Processes and Procedures and implement any required corrective action that has been Approved.
13-01-01-005-03 (Common)	3	The Hosting Supplier shall, where such information has not been provided within schedule 7.1 (Charges and Invoicing), provide a rate card for Project Management services in line with the Skills Framework for the Information Age (SFIA) to the Authority to decide Approval, within (40) Working Days of the TSA Effective Date.
		22.2 Quality Management
		22.2.1 Covers the planning and systematic activities implemented in a quality system so that quality requirements for a product or service will be fulfilled.
		22.2.2 The Service Requirements for Quality Management are listed below:
	2	**General requirements**
13-02-02-001-03	3	The Hosting Supplier shall perform quality assurance in accordance with the Authority's Policies, Processes and Procedures, or those of its nominated representative.

Requirement No.	Level	Requirement
13-02-02-002-03	3	The Hosting Supplier shall participate in the gate review process as set out in the Project Plan or as requested by the Authority or it's nominated representative.

Annex 1 – Social Value

Hosting Services
Schedule 2.1: Service Requirements
Annex 1: Sustainability and Social Value Requirements

Version Control			
Issue No:	Issue Date:	Issue Author:	Reason for Issue:
0.1	15 March 2022	Sharpe Pritchard	First draft
1.0	5 April 2022	Sharpe Pritchard	Final draft

1. INTRODUCTION

1.1 This annex 1 (Sustainability and Social Value Requirements) of schedule 2.1 (Service Requirements) covers:

1.1.1 social value;

1.1.2 carbon reduction, including the Carbon Reduction Plan.

2. PRINCIPLES OF SUSTAINABILITY AND SOCIAL VALUE

2.1 The Hosting Supplier acknowledges that the Authority places great emphasis on ensuring that public services the Authority is responsible for delivering are sustainable and deliver additional value in a wider community context, relevant to the services delivered.

2.2 The Authority is committed to achieving Net Zero by 2050 in the UK and wishes to ensure that contracts for public services include appropriate environmental management measures that are in effect and utilised during the performance of a contract.

2.3 In the event that a new service or a change to an existing service is made via the Change Control Procedure, the Hosting Supplier shall ensure that as part of its impact assessment the Hosting Supplier considers the sustainability and social value impact where appropriate.

3. SOCIAL VALUE

3.1 The Hosting Supplier recognises the UK Government's intention for public sector contracts to deliver social value to the communities we all work in. The Hosting Supplier supports this intent and has augmented its existing corporate social responsibility programme with a number of projects to realise greater social value.

3.2 Prior the Effective Date, the Hosting Supplier has established social value activities which include:

3.2.1 running a programme of STEM camps for children and the Hosting Supplier offered the collateral to a programme to train young offenders;

3.2.2 creating opportunities for businesses who train and employ former offenders in our supply chain (for example, to paint the Hosting Supplier's offices) and procure coffee for the Hosting Supplier's facilities from Redemption Roasters;

3.2.3 sponsoring local children's sports teams; and

3.2.4 running tree planting initiatives, including a strategic partnership with "Project Seagrass" which the Hosting Supplier believes could deliver a very substantial impact in Global sustainability.

3.3 From the Effective Date, the following further activities shall be carried out to meet Authority's social value requirement:

3.3.1 the Hosting Supplier and the Authority will establish a Quarterly forum to discuss social value and sustainability ("**Social Value Forum**") which shall meet in-person or virtually (with a preference to meet in person at least every other Quarter);

3.3.2 the Hosting Supplier will provide an update at the Social Value Forum to the Authority on:

3.3.2.1 the Hosting Supplier's social value projects across the Hosting Supplier's business and offer the Authority the opportunity to collaborate with the Hosting Supplier where appropriate; and

3.3.2.2 any opportunities to improve the social value or sustainability with regard to the ongoing Hosting Services.

3.4 The Hosting Supplier shall provide the Authority with a social value report on an annual basis throughout the Term. Such social value report shall provide an update on the social value activities undertaken by the Hosting Supplier and its Key Sub-Contract, REDACTED, in the previous twelve (12) months.

4. CARBON REDUCTION

4.1 The Hosting Supplier acknowledges that PPN 06/21 requires every entity bidding on UK public contracts worth over £5m to make a commitment to net zero by 2050 and produce a Carbon Reduction Plan.

4.2 As part of its global net zero commitment, the Hosting Supplier's UK business has received validation for its science-based targets (SBTs) and committed to achieve net zero greenhouse gas (GHG) emissions by 2026. The Hosting Supplier's published commitment is, therefore, some twenty-four (24) years ahead of the required UK Government target.

4.3 The Hosting Supplier shall report to the Authority on the Hosting Supplier's corporate Carbon Reduction Plan on an annual basis throughout the Term.

4.4 The Hosting Supplier's Carbon Reduction Plan as in place at the Effective Date is at appendix A to this annex.

APPENDIX A: CARBON REDUCTION PLAN

CGI Carbon Reduction Plan.pdf

End of schedule