APPLICATIONS AND HOSTING SERVICES

CALL OFF SCHEDULE 2

SERVICES

This Call Off Schedule consists of a Part A and a Part B. Part A contains the Service Requirements of the Customer and Part B contains the Supplier Service Descriptions.

PART A: SERVICE REQUIREMENTS

1. INTRODUCTION

1.1. This Part A contains the Customer's Service Requirements.

1.2. The Service Requirements under Part A of this Call Off Schedule are made up of three categories as follows:

1.2.1. Category 1 – General Requirements;

1.2.2. Category 2 – Operational / Technical Requirements; and

1.2.3. Category 3 – Agency Management Requirements.

1.3. Scope of the Services

1.3.1. Unless different Operational Service Commencement Dates are expressly identified in the Implementation Plan for any applicable parts of the Services, commencing on the Call Off Commencement Date the Supplier shall fulfil the following services, functions, responsibilities, requirements and deliverables (as the same may evolve during the Call Off Contract Period including adding, removing, supplementing, enhancing, modifying and/or replacing any services and/or activities or deliverables in accordance with this Call Off Contract or as otherwise Approved in writing by the Customer in accordance with the Change Control Procedures, from time to time):

1.3.1.1. the services, functions, responsibilities, requirements and deliverables that the Supplier is required to carry out as specified in Part A (Service Requirements) of this Call Off Schedule and the relevant Call Off Schedules and Appendices of the Call Off Contract;

1.3.1.2. any incidental services, functions, responsibilities, requirements and deliverables not specified in the Call Off Contract as within the scope of Supplier's responsibilities but that are reasonably and necessarily required for, or related to, the proper and timely performance and

provision of the services, functions, responsibilities, requirements and/or deliverables set out in Paragraph 1.3.1.1 above;

1.3.1.3. any services, functions, requirements, responsibilities and/or deliverables agreed pursuant to Call Off Schedule 14 (Change Control Procedure); and

1.3.1.4. subject to Paragraph 1.4 below, the services, functions, responsibilities, requirements and deliverables that the Supplier shall carry out as specified in Part B (Supplier Service Descriptions) of this Call Off Schedule, Call Off Schedule 8 (Security), Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel), and Call Off Schedule 10 (Business Continuity and Disaster Recovery)

(together, the "**Services**").

1.4. If there is any conflict between the scope of the services, functions, responsibilities, requirements and deliverables under: (i) Paragraphs 1.3.1.1 and 1.3.1.2 above; and (ii) Paragraph 1.3.1.4 above, the provisions of Paragraphs 1.3.1.1 and 1.3.1.2 above shall apply and prevail**.**

1.5. The Supplier shall meet and fulfil all of the Service Requirements in this Part A (and the Supplier confirms that the Supplier Solution set out in Part B of this Call Off Schedule meets and fulfils all of the Service Requirements in this Part A), as the same may evolve during the Call Off Contract Period and as they may be supplemented, enhanced, modified or replaced in accordance with this Call Off Contract, but excluding any services, responsibilities or functions that are expressly identified in the Order Form as the Customer's responsibility or a third party's responsibility.

1.6. If there is any conflict between the provisions of Part A of this Call Off Schedule and the provisions of Part B of this Call Off Schedule, the provisions of Part A of this Call Off Schedule shall prevail.

1.7. The Supplier acknowledges that as at the Call Off Commencement Date the Customer has appointed the Agency Manager to act in pursuance of the Customer's rights and to perform the Customer's obligations or functions under this

Call Off Contract. The Supplier shall follow the instructions of the Agency Manager in accordance with Category 3 of Part A of this Call Off Schedule.

2. BACKGROUND

2.1. The Department

2.1.1. The Crown Prosecution Service (CPS or the Customer) is the principle prosecuting authority for England and Wales, acting independently in criminal Cases investigated by the Police and other investigators including Her Majesty's Revenue & Customs and the Department of Work and Pensions. The Customer is headed by the Director of Public Prosecutions (DPP) and is one of the law officers' departments. The Director is superintended by the Attorney General who is accountable to Parliament for the Service. The Chief Executive of the Customer is responsible for the day to day running of Customer business.

2.1.2. The Customer was set up in accordance with the Prosecution of Offences Act 1985 to prosecute criminal Cases investigated by the Police in England and Wales. In undertaking this role, the Customer:

2.1.2.1. Advises and assists the Police during the early stages of investigations;

2.1.2.2. Decides on the appropriate charge, in all but minor Cases;

2.1.2.3. Keeps all Cases under continuous review and decides which Cases should be prosecuted;

2.1.2.4. Prepares Cases for court and will either conduct advocacy in court, using an in-house lawyer resource, or instruct a self-employed advocate, generally from the criminal bar; and

2.1.2.5. Provides information and assistance to victims and prosecution witnesses.

2.1.3. The Customer is at the centre of the Criminal Justice System whereby police and other investigators address allegations and incidents and work with Customer staff to determine appropriate charges; the prosecution is prepared and presented in the Courts by Customer teams who also support victims and

witnesses; and, at the close of proceedings, convicted persons are passed into the custody of Prisons and Offender Management agencies.

2.1.4. The Customer comprises fourteen (14) geographical Business Areas across England and Wales which administer smaller Operational Units, and CPS Direct which provides a twenty four (24) hour service of advice on prosecution charges to the police and other investigators. There are also three (3) central Casework divisions that handle the most serious, complex or sensitive prosecutions covering specialist fraud, special crime and counter terrorism and organised crime. Finally, the Department has headquarters, corporate service and operations management business functions.

2.1.5. The Customer employs approximately 6,500 people, including some 2,200 Crown prosecutors and 3,600 paralegals/Case administrators, and headquarters staff, and prosecutes approximately 600,000 Cases each year in magistrates' courts and about 100,000 Cases in the Crown Court. In addition to its staff working on Customer Premises, the Customer's technology infrastructure supports some 100 Police officers working from Police stations and Customer Premises and Customer staff in CPS Direct that work from home and/or the Customers Premises. The number of Users should be estimated as around 6,500 for the Call Off Contract Periodunless otherwise stated by the Customer.

2.1.6. The Customer website (www.cps.gov.uk) provides further information about the organisation, including the Customer's Annual Report and Accounts as referenced in Part A of Table 10 of this Call Off Schedule.

2.2. Infrastructure

2.2.1. The Customer's Application infrastructure is made up of a wide range of hardware and software components which are hosted principally at the Former Supplier's data centres. The data associated with the Business Critical Systems is hosted also resides at the same data centres.

2.2.2. The Scope of the services shall include the provision of application support and the hosting of associated data for:

2.2.2.1. Business Critical Systems;

2.2.2.2. Non Business Critical Systems of High Importance; and

2.2.2.3. Non Business Critical Systems of Medium Importance.

2.3. In this Call Off Schedule, where the provisions of Parts A and B of this Call Off Schedule use any of the following terms, such terms shall be construed as the capitalised terms set out in Call Off Schedule 1 (Definitions) save where the context provides otherwise:

2.3.1. applications;

2.3.2. assets;

2.3.3. availability;

2.3.4. component;

2.3.5. incident;

2.3.6. software.

CATEGORY 1: GENERAL REQUIREMENTS

#	Requirement
APPS/R/GREQ/001	The Supplier shall deliver all Services in accordance with the Call Off Terms of the Call Off Contract, including the Standards.
APPS/R/GREQ/002	The Supplier shall, wherever possible, use Standards-based solutions. This shall apply to technical solutions as well as management and operational interactions between the Supplier and the Agency Manager (e.g., operating models based on COBIT (Control Objectives for Information and Related Technology), TOGAF (The Open Group Architecture Framework), and ITIL (Information Technology Infrastructure Library)).
APPS/R/GREQ/003	To ensure that maximum process efficiency and data quality are obtained in relation to the Services, the Services shall be automated by the Supplier wherever there is the opportunity to do so. The Supplier shall ensure that the Services shall be designed to capture data only once, thus minimising the need for manual data capture and input. All data shall be validated by the Supplier on input.
APPS/R/GREQ/004	The Supplier shall wherever possible use simplified assurance and payment processes when invoicing the Customer.
APPS/R/GREQ/005	Save as otherwise expressly stated in the Call Off Contract, the Supplier shall ensure that, upon request from the Customer, certain of: (i) the Supplier's Personnel; (ii) and any of the Key Personnel; and/or (iii) other relevant persons identified by the Customer that the Customer wishes to meet, shall attend workshops or meetings with the Customer and/or any other Related Supplier as the Customer reasonably deems necessary given the circumstances.
APPS/R/GREQ/006	Where the Supplier fails, or becomes aware that it is likely to fail to comply with any obligation of this Call Off Contract and such failure may impact on the performance of the Services by the Supplier (including the Service Levels), the Supplier shall, as soon as is reasonably practicable, notify the Customer of such failure or likely failure.
APPS/R/GREQ/007	The Supplier shall notify the Customer when it becomes aware of an actual or potential event that may pose a risk to the Services and shall provide to the Customer all necessary details and information of such event.

#	Requirement
APPS/R/GREQ/008	The Supplier shall comply with the Data Protection Legislation and data protection provisions set out in the Call Off Contract, including in relation to the Processing of the Personal Data controlled by the Customer.
APPS/R/GREQ/009	The Supplier shall provide support to the Related Suppliers including, where necessary, access to resources, the Supplier System, Software and any materials as required, and to deal with security and/or compliance issues, assessments and actions. Any work arising under this requirement that is outside the scope of the PPPs would be subject to Call Off Schedule 14 (Change Control Procedure).
APPS/R/GREQ/010	The Supplier shall perform the Services in accordance with Clause 7/8 of the Call Off Terms and this Call Off Schedule. The Supplier shall use ITIL (Edition 2011 or the then current version of ITIL) based processes and perform the Services in accordance with industry based best practice and, if required, the Supplier shall demonstrate this to the satisfaction of the Customer.
APPS/R/GREQ/011	The Supplier shall adhere to the Agency Manager provided common Standards for interfaces to the ITSM Toolset for the management of Services events across the Service Management Lifecycle. Amendments to such common Standards that result in a material change to the Supplier Solution shall be subject to Call Off Schedule 14 (Change Control Procedure).
APPS/R/GREQ/012	The Supplier shall ensure that Processes for all ITIL functions are aligned (to the work instruction procedural level) with the Policies, Processes and Procedures set out by the Customer by the end of Implementation. The Supplier shall ensure that all hand-over and hand-back points and Dependencies between: (i) the Supplier and the Customer, (ii) the Supplier and the Agency Manager; (ii) the Supplier and Related Suppliers are clearly set out in the SOM. Amendments to such Policies, Processes and Procedures that result in a material change to the Supplier Solution shall be subject to Call Off Schedule 14 (Change Control Procedure).
APPS/R/GREQ/013	The Supplier Solution shall be implemented in a modular and commoditised way, allowing for flexible and scalable Services that can be updated and replaced with minimal disruption to the Customer.
APPS/R/GREQ/014	The Supplier shall facilitate process efficiency by choosing automation over manual intervention and empowering the business to self-serve, subject to such automation being Approved by the Customer in advance.

#	Requirement
APPS/R/GREQ/015	The Supplier shall ensure that the Supplier Solution shall have a documented design and be implemented such that it has optimum scalability, and for process and technology integration with other Related Suppliers. Any material changes required to the Supplier Solution arising out of such process and technology integration with Related Suppliers shall be subject to Call Off Schedule 14 (Change Control Procedure).
APPS/R/GREQ/016	The updating of Service event data shall occur immediately or in sufficient time to enable effective Management Information to be produced and acted upon in accordance with Service Levels, Service Level Performance Measures, and Key Performance Indicators for the Services.
APPS/R/GREQ/017	The Supplier shall ensure that all necessary support is provided to the Customer, or any Auditor assigned or appointed by the Customer, to audit any aspect of the Services provided by the Supplier.
APPS/R/GREQ/018	The Supplier shall annually assess the maturity of the Services using the HMG Green ICT Maturity Assessment Model and the Supplier shall provide the findings to the Customer within thirty (30) Working Days of each annual anniversary of the date of Achievement of the Final Operational Services Commencement Date.
APPS/R/GREQ/019	The Supplier shall bear the cost of decommissioning, collection and disposal of Supplier Equipment.
APPS/R/GREQ/020	The Supplier shall provide to the Customer access for validation purposes to all raw data and access on demand to all the Supplier's reporting tools.
APPS/R/GREQ/021	The Supplier shall provide a SOM in accordance with Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel) and update it in consultation with the Customer from time to time and baseline it annually on each anniversary of the Call Off Commencement Date.
APPS/R/GREQ/022	The Supplier shall act as the operational agent on behalf of the Customer for Crown Hosting services procured by the Customer. The scope of such work shall be as set out in the applicable procurement contract with Crown Hosting which shall be agreed (such agreement not to be unreasonably withheld or delayed) in advance with the Supplier.

CATEGORY 2: OPERATIONAL/ TECHNICAL REQUIREMENTS

Category 2 of Part A of this Call Off Schedule provides the operational and technical requirements of the Customer in relation to the Services.

This category is broken down into two main sections:
1. Data Hosting; and
2. Application Support.

Background and Overview – Data Hosting

1. Data Hosting

The Supplier shall provide and support a Private or Community Cloud environment to the Customer. The terms Private or Community Cloud refer to the NIST Standards. Definitions of these terms are:

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.

1.1 Data Hosting

Reference ID	Requirement
APPS/R/HOST/001	The Supplier shall provide and support a Private or Community Cloud environment to the Customer.
APPS/R/HOST/002	The Supplier shall ensure data centres used in the provision of the service are registered as participants under the EU Code of Conduct for Data Centres Energy Efficiency.
APPS/R/HOST/003	The Supplier shall provide the following infrastructure within their data centres a. Infrastructure application servers b. Database management servers c. Authentication servers d. Application servers e. Management servers f. Backup servers g. Unix servers (where required) h. Data Storage for both structured and unstructured CMS data.

Reference ID	Requirement
	i. Tape Library(s)
APPS/R/HOST/004	The Supplier shall Implement, maintain and support standard physical server builds sized by CPU, number of cores, RAM and interfaces, to be offered in small, medium, and enterprise builds in support of the Services.
APPS/R/HOST/005	The Supplier shall Implement, maintain and support standard virtual server builds sized by CPU, number of cores, RAM and interfaces, to be offered in small, medium, and enterprise builds in support of the Services.
APPS/R/HOST/006	The Supplier shall provide connectivity into the Customer WAN cloud and external networks such as the CJX and PSN networks.
APPS/R/HOST/007	The Supplier shall provide fail over resilience between data centres.
APPS/R/HOST/008	The Supplier shall provide backup and recovery to tape and disk storage.
APPS/R/HOST/009	The Supplier shall provide resilient power to all data centre hosted servers and infrastructure equipment.
APPS/R/HOST/010	The Supplier shall provide management information & monitoring of all servers.
APPS/R/HOST/011	NOT USED
APPS/R/HOST/012	The Supplier shall provide the ability to offload files, media, images and other agreed objects from compute resources.
APPS/R/HOST/013	The Supplier shall provide resilient data centre infrastructure with no single point of failure.
APPS/R/HOST/014	The Supplier shall ensure the replication of data and VMs to the secondary site to provide business continuity in the event of a catastrophic failure at the primary site.
APPS/R/HOST/015	It shall be possible for the Customer to present their own connections and offer a secure remote access solution that allows assured VPN access to the elevated OFFICIAL domain.
APPS/R/HOST/016	When the Services (or part thereof) is no longer required a backup of Customer Data shall be provided on request in a mutually agreed extract format. Where appropriate, this shall include an image of the virtual machine.
APPS/R/HOST/017	NOT USED
APPS/R/HOST/018	The Supplier shall provide Protected Internet connectivity for the Customer by a direct internet connection from the Supplier's data centres.
APPS/R/HOST/019	Subject to the provisions of Call Off Schedule 9 (Software and Assets) relating to support and/or upgrade constraints, the Supplier Solution shall support disparate technologies of varying age (and in some instances, technologies that no longer have vendor support) as such technologies and ages are identified in Call Off Schedule 9 (Software and Assets).
APPS/R/HOST/020	The Supplier shall host some case materials (particularly in relation to large cases) outside of the CMS.
APPS/R/HOST/021	The Supplier shall host Federated Active Directory services as

Reference ID	Requirement
	needed to connect with Office 365 services hosted on the Azure platform.

Background / Scope: The Hosting of data within a Supplier's data centre is primarily done through a cloud or on premise environment. The data and Applications are migrated from the existing data centre to the hosted data centre, with the service provider being responsible for providing resilience, power, backup, recovery and other such functions.

1.2 Backup and Recovery

Reference ID	Requirement
APPS/R/BREC/001	The Supplier shall safeguard Software and Customer Data against loss or damage. In particular, the Supplier shall: a. take copies of all new and changed Software and Customer Data on at least a daily basis and restore the most recent versions in the event of a failure; b. maintain full copies of all Software and Customer Data regularly and restore the most recent versions where necessary; c. maintain a log of all backups to enable speedy access and restoration; d. provide all appropriate protection including up-to-date virus protection; and e. restore Customer Data and User-specific Applications upon request from a User, e.g. where a User has inadvertently deleted or corrupted Customer Data.
APPS/R/BREC/002	In the event of the loss of a Business Critical System, the Supplier shall ensure that Software and Customer Data are fully restored to the state at the point of failure within the relevant Service Levels.
APPS/R/BREC/003	The Supplier shall monitor and verify all backups. This will ensure that, in the event of system failure all Non Business Critical System data can be restored from these backups. Backup of any data held away from the file servers (i.e. on a User Device) will be the responsibility of the User.
APPS/R/BREC/004	The Supplier shall provide resilient data centre infrastructure with no single point of failure.
APPS/R/BREC/005	On request by the Customer, the Supplier shall restore the most recent version of Customer Data to a point not exceeding one (1) Working Day previously.
APPS/R/BREC/006	The Supplier shall provide redundant disk architecture for Business Critical Systems such that the loss or failure of a part of the architecture does not cause loss of data for that Service i.e. the data is stored in multiple locations. In addition, the Supplier shall perform a daily backup of Customer Data held on Business Critical Systems
APPS/R/BREC/007	The Supplier Solution shall promote data backup to the cloud, as a location-agnostic (UK-based), secure and cost-effective alternative to storing backups on unreliable tape media or expensive local disk

Reference ID	Requirement
	solutions.
APPS/R/BREC/008	The Supplier shall enable the transfer of valuable but seldom used Customer Data to a cost efficient, reliable and secure repository, to migrate seldom accessed data to more cost effective storage solution.
APPS/R/BREC/009	The Supplier Solution shall promote archiving to the cloud as a means of storing valuable but seldom used data to a cost-effective, reliable and secure cloud storage repository via PSN, the internet and other networks.

Background / Scope: A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. The primary purpose is to recover data after its loss, be it by data deletion or corruption.

2. Application Support

The Application Support Service Requirements can be categorised as:

A. Business Critical Systems;
B. Non Business Critical Systems of High Importance;
C. Non Business Critical Systems of Medium Importance;
D. General Operational/ Technical Requirements; and
E. Service Requirements.

A Business Critical Systems

A.1 Background and Overview

The department's Business Critical Systems are (i) the Case Management System, (ii) Witness Management System, (iii) Management Information System, and (iv) Evidence Management System. These systems are supported by a series of other Applications that support mobile working, systems security and administration, etc.

(i) CMS

CMS is a centralised, bespoke Case Management System that was introduced in 2003 and replaced the many separate case management systems established over the years within the individual Customer Business Areas. CMS is the Customer's business critical application supporting the core business process of prosecuting criminal cases. It is a national cCase tracking and management system providing case management for criminal cases dealt with in the Magistrates' or Crown courts or courts of Appeal. It supports the prosecution process by helping Users to manage the progress of a case file throughout its lifecycle from receipt to final conclusion.

There are approximately 6,000 Users of CMS. The application employs a thin client architecture using IE11, DHTML, JavaScript and MS Office at the client side, IIS, .NET and ASP.Net on the middle tier and Oracle 11g at the back end.

The core CMS system is divided into the following tiers:

a. Browser-based User interface with some client side controls;

b. Web servers to deliver the application using MS .NET technology (IIS, ASPs etc.); this tier does not implement the business logic;

c. Middle tier implementing the business logic;

d. Data tier containing the case file metadata and content

The ability to generate structured PDF electronic document bundles from case documents held in CMS is available. General functionality supporting Users emailing case information from within CMS is also available.

Physically all tiers and the structured bundling application are to be implemented within the Supplier's data centres except the top tier. The top tier (browser) is implemented within the Customer Premises using the office infrastructure. The infrastructure makes use of VM Ware to virtualise x86-64 based application servers.

In 2015 'The Prosecutor App' was introduced to support prosecutors in court including recording the outcome of hearings. This application communicates with the central CMS system using web services when online and stores information locally when offline. It also provides the capability for guilty-plea at first hearing cases to be automatically finalised on CMS.

Functionality changes – the Customer periodically requires CMS functionality updates and these are implemented by regular releases throughout the year. The primary drivers for these changes span the following areas:

1. legislative changes to the way the Customer works
2. business optimisation of processes within the Customer, including User led efficiencies
3. changes to enable the Customer to work more effectively with other IT systems and platforms across the Criminal Justice System e.g. HMCTS and Police systems

The frequency and nature of these changes is based upon business demand and prioritisation. The changes are expected to reduce as a result on the introduction of Common Platform; however a number of changes will be required in the interim to support this programme under area 3 (above).
To address area 2 a series of more modern screens are currently being developed for some areas of CMS, with a new User interface.

CMS key functions.

Information Capture – the CMS provides User interface screens to allow Users to register details of a case and to update case information when necessary. The system also supports electronic interfaces for the exchange of structured data and unstructured evidential material with the Courts and Police.

Automated Case Progression / Time Limit Monitoring – the Customer prosecutes cases using a defined set of processes; for example advice, registration and review. There is no single fixed route for a case through the prosecution process, though there are a number of activities usually defined through legislation or procedural rules that will apply. The rules that govern the progression of a case are used to configure a rules engine. The rules engine is responsible for creating tasks that prompt Users to perform actions at a given time. The system calculates and monitors time limits and alerts the User to approaching deadlines.

Search Facilities – the CMS provides facilities to search for and retrieve case information. Search facilities include the ability to search for: matching defendants based upon their

names, cases based on the barcode on the case label and cases identified by case information such as URN.

Assisted Production of Outputs – the Customer produce a series of documents for presentation to the courts, the defence, the Police and for use by the Customer in court. The CMS will assist in the production of these documents by providing facilities to automatically insert information
stored in the CMS into standard document templates. Operational Units may override certain nationally provided templates with their own local versions. These outputs can also include structured bundles of documents in the form of a PDF document that is paginated and bookmarked.

Management of Electronic Documents – the CMS provides facilities to store and associate electronic documents with case files. Facilities are provided to view and print electronic documents at the request of the User.

Management of Electronic Records – the CMS provides functionality to meet requirements for electronic records management of case material. This includes the archiving and destruction of electronic case files.

Case Reporting – the CMS provides functionality to report on case information for cases that are currently live. These reports will be based on the data in the CMS database at the time that they are run. A typical report of this type might be a report on current lawyer workload at a given Customer unit.

Configuration – the CMS provides an interface to allow the management of configuration information by Users (e.g. data administrators with Designated Access Rights), such as the setting of local flags available for monitoring cases. However, Users are not permitted to make changes to the rules that control case progression. Where appropriate the system will allow for regional configuration of data and regional variation in the case progression rules.

User Interface – the CMS provide a User interface that has been developed alongside a business process modelling exercise through prototyping workshops. A series of modern screens are currently being developed where appropriate to address functionality changes.

CMS Processes

For the structural requirements for CMS, please refer to the table in Annex 1 of Part A.

Case management processes used include, but are not limited to:

1. Papers Received
2. Case Registration
3. Allocation
4. Review
5. Advance Information
6. Tape Management
7. Preparation of Court Lists – Magistrates' Courts
8. Preparation of Court Lists - Crown Court
9. Preparation for Court Attendance - Magistrates' Courts
10. Preparation for Court Attendance – Crown Court

11. Preliminary Hearings – Magistrates' and Crown Courts
12. Post Court Action
13. Trial Preparation - Magistrates' Courts
14. Trial Preparation - Crown Court
15. Trial Preparation – Witnesses: Magistrates' Courts
16. Trial Preparation – Witnesses: Crown Court
17. Trial Overview
18. Sentencing Hearings
19. Sentencing Hearings: Previous Convictions
20. Sentencing Hearings: Pre-Sentence Reports
21. Sentencing Hearings: Unduly Lenient Sentence
22. Sentencing Hearings: Committals for Sentence
23. Sentencing Hearings: Appeals against Sentence to the Crown Court
24. Appeals against Conviction to the Crown Court
25. Appeals to the Court of Appeal
26. Applications and Appeals to Higher Courts (minor process)
27. European Court of Human Rights (minor process)
28. Bail Applications
29. Bail Applications: Appeal by the Prosecution against Grant of Bail
30. Bail Applications: Warrants and Failure to Surrender to Bail
31. Bail Applications: Breach of Bail Conditions
32. Transfer Proceedings
33. Archiving
34. Youth Offenders
35. Custody Time Limits
36. Selection and Instruction of Advocates
37. Court Coverage
38. Disclosure of Unused Material
39. Disclosure of Unused Material: Sensitive Material
40. Miscellaneous Proceedings (minor process)

An overview of the functionality of each CMS sub system can be found in the document titled **D133_453001_04 (14.00) CMS FS Functional Overview**

(ii) WMS

For the structural requirements for WMS, please refer to the table in Annex 1 of Part A.

The Witness Management System (WMS) is an extension to CMS which uses the same architecture and shares a common database and document repository with CMS. The WMS application provides a different User interface using the same technology stack as CMS. WMS was set up as part of the No Witness No Justice (NWNJ) initiative. WMS provides case management support for Witness Care Units and gives witnesses a single point of contact throughout the prosecution process. These units are jointly staffed by Police and Users and there are approximately 1,800 Users of WMS. Some of the units are connected directly to the Customer network infrastructure whilst others are part of the police infrastructure.

The WMS application is made available to Users across the Customer Network and to Police Users via the CJX network. The Police Users access the WMS web site across their own force networks and then ultimately through their gateway onto the CJX. To provide further access controls on the Sensitive Information held in WMS a two factor authentication

mechanism has been implemented using the same ActivCard technology employed for the Customer remote access system.

The primary difference between CMS and WMS is that a large proportion of the Users are located in police buildings and use police infrastructure.

Key WMS functions

The following is a list of the key functions provided by the WMS

Search Facilities – the WMS provides facilities to search for and retrieve case information from CMS. Search facilities include the ability to search for: matching defendants based upon their names, matching the Witness Care Officers (WCO), the witness or the victim and cases identified by case information such as URN.

Allocation – The WMS allows CMS cases to be allocated to the Witness Care Officers.

User Interface – the WMS provides a User interface to display existing CMS case details on screens specific to WMS.

Assisted Production of Outputs – the Witness Care Units (WCU) produce a series of documents for communicating with the witnesses. An example would be the production of a letter informing the witness of the outcome of a hearing. The WMS assists in the production of these documents by providing facilities to automatically insert information stored in the CMS and WMS into standard document templates. The WMS uses reminders to support the work.

Information Capture – the WMS provides User interface screens to allow Users to update case information when necessary. The WMS provides functionality to report on witness information for cases. Reports are run quarterly to provide victim and witness details so that satisfaction levels may be monitored.

(iii) MIS - Management Information Systems

For the structural requirements for MIS, please refer to the table in Annex 1 of Part A.

MIS provides statistical and summary information on the progress of cases within Customer. This is based on Business Objects Web Intelligence and has around 200 Users with Designated Access Rights. The MIS is a database, separate from the CMS, which stores case information extracted on a nightly basis from the CMS. The extraction process anonymises data in the sense that personal information is not extracted, e.g. for a defendant, gender and ethnicity will be extracted but not name and address details. SAP Business Objects is the reporting tool used to structure, analyse and report on the data set.

External Interfaces

The CMS and WMS have interfaces with external organisations. These interfaces enable the exchange of structured case data and unstructured evidential material with police force and court systems.

Examples of such interfaces are:

a. An interface to the police case management systems via the CJS Exchange that allows for the exchange of information between Compass CMS and the police case management systems.

b. An interface to the Ministry of Justice (MoJ) Digital Case System (DC S aka Caselines) from CMS (and in the summer of 2017 with EMS) that enables the evidential material for Crown Court cases to be published in DCS.

c. An interface to the HMCTS Court Store is in place. This interface allows CMS to publish bundles and other documents, together with supporting case data, to the Court Store for use by HMCTS or other parties.

Further detail is set out in this document.

(iv) Evidence Management System (EMS)

EMS is an electronic storage and transmission facility to store evidential material and case correspondence (some of which may become evidential material) and to enable searching and management of the material.

Case Material will include a range of documents and other items, including photographs and potentially multimedia exhibits.

EMS is designed to assist in the management of cases with large volumes of digital exhibits and correspondence, in particular those cases handled by the central and complex casework units. It also produces court bundles and links to some of the Customer's partner agencies.

The system is built using Documentum xCP and is composed of several EMC software components and one non-EMC component. The non-EMC component, Brava, is developed by IGC software and is resold by EMC to integrate with the Documentum xCP platform and provide document viewing functionality.

A.2 Business Critical Systems – Functional Requirements

The requirements set out under this section cover:

#	**Business Critical System**
1	CMS, WMS, MIS
2	EMS
3	SharePoint
4	Not used
5	Active Directory
6	Blackberry Enterprise Server

7	Email services
8	Group Policy Objects
9	Juniper Remote Access
10	Solidus access
11	Two factor authentication (Active Card) systems

Note: The functional requirements for the application support of CMS, WMS and MIS Business Critical Systems are extensive. This is because CMS, WMS and MIS have been developed specifically for the Customer, and need to be provided exactly as set out within the functional specifications referred to in this Call Off Schedule. The other systems are COTS products and consequently do not need as much detail. As mentioned above, for the structural requirements for CMS, WMS and MIS please refer to the table in Annex 1 of Part A

1. CMS, WMS, MIS

Reference ID	Requirement
APPS/R/GFUNC/001	The Supplier shall allow the Customer to add or remove Business Critical Systems using the Change Control Procedures.
APPS/R/GFUNC/002	The Supplier will be responsible for seeing all data centre infrastructure, Business Critical Systems, Non Business Critical Systems, and other infrastructure service related incidents through to resolution.

1.1 General Case Facilities (CG)

Reference ID	Requirement
APPS/R/GCASE/001	The following will apply to the functional specifications in this Section 1 (i.e., 1.1 to 1.49 but excluding Section 1.48), Apps/R/GENNFUN/017 and APPS/R/GENNFUN/019 below: • The Supplier will provide CMS / WMS / MIS functionality in accordance with the Functional Specifications named in the VDR at the time of RFP issue. The Supplier and the Customer shall work together as part of Services governance. If it is demonstrated that the Functional Specifications were inaccurate at the time of RFP issue or updates to CMS / WMS / MIS have been made since RFP issue, any resulting changes to CMS / WMS / MIS shall be subject to the Change Control Procedure.
APPS/R/GCASE/001A	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CG1 (18.00) CMS FS Cases subsystem

Reference ID	Requirement
	• 453001_08_CG2 (18.00) CMS FS Cases subsystem

Background / Scope

The General Case Facilities sub-section contains case-related functionality which is not specifically tied to a functional area. The screens, functions and rule sets within the sub-section are used by other sub-sections within the Cases subsystem and by other subsystems within CMS.

This sub-section includes the Case Details screen (CG01S) which is the primary screen in CMS for viewing and amending case details. This screen also uses functionality in the Case Review (CR) and Hearing Preparation (CP) sub-sections to provide facilities for reviewing and recording review comments, and for progressing hearing preparation.

The Case Details screen itself consists of a number of tabs, each displaying a related set of data which is linked to the case.

Below is a list of other general case facilities.

1. General Case Facilities (CG)
2. CG24F: Calculate Charge CTL
3. CG25F: Define Leading CTL for Case
4. CG26S: Contacts (Case Details) Screen
5. CG27F: Save Contact Function
6. CG28R: Calculate CTL Details
7. CG29F: Finalise Case Function
8. CG30R: Case Finalised Rule Set
9. CG31F: Delete Case Function
10. CG32F: Reactivate Case Function
11. CG33S: Case Summary Screen
12. CG34S: Case Status Screen
13. CG35F: Add Organisation Contact to Case Function
14. CG36F: Add Person Contact to Case Function
15. CG37F: Remove Organisation Contact From Case Function
16. CG38F: Remove Person Contact From Case Function
17. CG39F: Remove Defendant's Legal Representation Function
18. CG40F: Remove Counsel from Case Function
19. CG41S: New Contact Screen
20. CG42S: Merge Witnesses Dialogue Screen
21. CG43F: Merge Witnesses Function
22. CG44F: Delete Witnesses Function
23. CG45S: Advice Case Details Screen
24. CG46S: Advice (Advice Case Details) Screen
25. CG47F: Save Advice
26. CG48R: Communications Saved Rule set
27. CG49S: Select Advice Mode Dialog
28. CG50R: Advice Mode Selected Rule set

29. CG51R: Advice Saved Rule Set
30. CG52S: Record Case Dates Screen
31. CG53R: Case Dates Recorded Rule set
32. CG54R: No Longer Used
33. CG55S: No Longer Used
34. CG56R: Info Read Rule set
35. CG57S: Browse Case Screen
36. CG58S: Destroyed Case Summary
37. CG59S: CTL Details Screen
38. CG60R: Handle CTL Status Change Rule set
39. CG61R: Handle Conditional Remand Changes Rule set
40. CG62F: Save Offence Change
41. CG63R: Case Reactivated Rule set
42. CG64F: Store Case Monitoring Status
43. CG65F: Retrieve Current Case Monitoring Status
44. CG66S: Print Case Screen
45. CG67F: Print Case Evidence Function
46. CG68F: Update Pending Deletion Status
47. CG69S: View Email Screen
48. CG70F: Print Email Function
49. CG71F: Print Witness Availability Report Function
50. CG72S: Sentence Notes Screen
51. CG73S: Bail Notes Screen
52. CG74F: Add Court Contact to Case Function
53. CG75S: Print Witness Expense Form Labels Screen
54. CG76F: Print Witness Expense Form Labels Function
55. CG77S: Action Plan Screen
56. CG78F: Save Action Plan Data
57. CG79S: File Build/Action Plan Screen
58. CG80F: Retrieve File Build/Action Plan Options
59. CG81F: Store File Build/Action Plan Options
60. CG82S: Victim Witness Deletion/Rejection Screen
61. CG84F: Add Defendants to Merge
62. CG85F: Delete Action Plan Data
63. CG86F: Merge Defendants Checks
64. CG87F: Merge Defendants
65. CG88R: Merge Defendants Rule Set
66. CG89S: Print Review Screen
67. CG90F: Check Witness Victim is modified
68. CG91F: Set Witness Victim Update Audit Attribute Values
69. CG92F: Update Pending Witness Contact Data
70. CG93S: Update to Witness Contact Details Screen
71. CG94F: Display Witness Victim Audit Details
72. CG95R: Victim/Witness Deletion Request Rule Set
73. CG96R: Witness/Witness Selection Saved Rule Set
74. CG97R: VPSISB Status Check Rule Set
75. CG98F: Check Court Live Status
76. CG99F: Determine Eligible Hearings for Bundle
77. CG100S ‘Link Bundle to Hearings’ Popup

The detailed functional specification for the list above is set out within the following documents:

a. 453001_08_CG1 (18.00) CMS FS Cases subsystem;
b. 453001_08_CG2 (18.00) CMS FS Cases subsystem

The Supplier shall continue to deliver such functionality as set out in the detailed functional specification.

1.2 General Case Facilities (WCG)

Reference ID	Requirement
APPS/R/GCASEW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCG1 (18.00) WMS FS Case subsystem • 453001_08_WCG2 (18.00) WMS FS Case subsystem

Background / Scope: The General Case Facilities sub-section contains case-related functionality which is not specifically tied to a functional area. The screens, functions and rule sets within the sub-section are used by other sub-sections within the WMS Cases subsystem and by other subsystems within WMS.

1.3 Case Allocation (CA)

Reference ID	Requirement
APPS/R/CASAL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CA (18.00) CMS FS Cases subsystem

Background / Scope: Allocation is defined within the Case Management System as the association of individuals with a case. It establishes individual responsibility for a case, and as such acts as a formal method for a unit head to delegate the responsibility for work on a case to individuals in his or her unit.

This sub-section of the Cases subsystem provides the screen through which Users can allocate resources to cases, plus rule sets and functions to support the maintenance of allocation to cases, the creation of tasks to prompt for manual allocation of resources to cases, and the handling of resource re-allocation following the transfer of a case between Customer units.

1.4 Case Allocation (WCA)

Reference ID	Requirement

Reference ID	Requirement
APPS/R/CASALW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCA (18.00) WMS FS Cases subsystem

Background / Scope: Allocation is defined within WMS as the association of individual Witness Care Officers (WCOs) with a case. Allocation establishes individuals' responsibility for a case.

This sub-section of the Cases subsystem provides the 'Allocate Case' screen through which Users can allocate resources to cases, plus rule sets and functions to support the maintenance of allocation to cases and the handling of resource re-allocation e.g. following the transfer of a case between Customer Operational Units on CMS.

1.5 Structured Bundling (CB)

Reference ID	Requirement
APPS/R/SBUND/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CB (18.00) CMS FS Cases Bundles

Background / Scope: The User is able to identify the type of bundle, identify the Defendants and then prepare ordered bundles from selected documents and files sourced from within and outside CMS.

During the preparation of the bundle, the User is able to add new sections and sub-sections, identify whether or not the section or sub-section should be paginated and request sub-pagination or multi-pagination.

1.6 Counts and Indictments Preparation (CC)

Reference ID	Requirement
APPS/R/COUN/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CC (18.00) CMS FS Cases subsystem

Background / Scope: The Counts and Indictments Preparation sub-section of the Cases subsystem includes the functionality required to build counts* and to select counts to include in an indictment.

The Build Indictment Screen (CC01S) allows the User to

a. Build counts using a template;
b. Select counts to be included in an indictment;
c. Order the defendants within the indictment;
d. Trigger the production of an indictment that will be dispatched from the Communications tab.
e. Revert a count to its state when it was lodged by the User, or accepted at court.

(* 'counts' is used in a legal context to mean the charge, or charges, being put to a Defendant.)

1.7 Case Pre-Charge Decision (CD)

Reference ID	Requirement
APPS/R/PCHARG/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CD (18.00) CMS FS Cases subsystem

Background / Scope: The Criminal Justice Bill 2003 introduced legislative changes that extended the role of the Customer in the pre-charge phase of cases. In particular Customer lawyers now work more closely with the police and have become responsible for making the decision on what to charge a suspect with in certain cases.

The basic objective of the scheme is to ensure that when a defendant is charged, the charges are appropriate (i.e. accord with the available evidence) and the case is suitable to progress to court for a prosecution. This should lead to a number of benefits across the Criminal Justice System, in particular Defendants are more likely to plead Guilty, the average number of hearings required to complete the case should be less, and charge discontinuance rates should reduce.

When a case is referred to Customer for a pre-charge decision, there are a number of possible outcomes:

a. the case is not to proceed to a prosecution in court, e.g. could be effectively dealt with by a Police Caution or Warning;
b. based on the evidence presented, the lawyer is able to make a decision on what to charge the suspect with, and the police then charge the suspect with the case expected to proceed to a prosecution in court;
c. based on the evidence presented, the lawyer is able to make a decision on what to charge the suspect with, but considers that it is more valuable to conditionally caution the suspect. If the suspect complies with the conditions of this caution within the stated timeframe he/she will avoid prosecution. If instead he/she fails to comply then the prosecutor will again consider the case and may decide to proceed to prosecution the second time round.
d. based on the evidence presented, the lawyer is unable to able to make a decision on what to charge the suspect with, and for example suggests further evidence the police need to gather before they can decide what charges are suitable.

1.8 Case Progression Functionality (CE)

Reference ID	Requirement
APPS/R/CASEPRG/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CE (18.00) CMS FS Cases subsystem

Background / Scope: Progressing a case is via a few key screens. The Directions for Unit screen is the main screen that an Operational Unit uses to carry out case progression work. It may be accessed at any time from the menu bar by selecting the 'Directions for Unit' option from the 'Directions' top level menu item.

The screen lists the directions that apply to cases owned by the User's Operational Unit. By default the screen lists directions that require the most immediate attention; these are directions that are near to, or have passed, their due date and are colour coded. This helps to ensure that the necessary case preparation work is carried out before a hearing occurs. The screen includes a search pane with a range of filter options to allow the User to search for those directions which are of interest to them, such as directions with outstanding work on them.

1.9 WMS Case Progression Functionality (WCE)

Reference ID	Requirement
APPS/R/CASEPRGW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCE (18.00) WMS FS Cases subsystem

Background / Scope: The Effective Trial Management Programme (ETMP) was established to improve the effective management of criminal cases, following a review of the Criminal Courts in 2001. It focused on improving case preparation and progression. Case Progression functionality has been introduced into CMS and WMS to support ETMP.

1.10 Confiscation Cases (CF)

Reference ID	Requirement
APPS/R/CONFC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CF (18.00) CMS FS Cases subsystem

Background / Scope: The Confiscation Cases section of the Cases subsystem details the Manage Orders screen and functions used to record details of orders relating to the confiscation elements of charge cases. The Manage Orders screen allows the User to add, edit and delete the following types of order for Defendants:

a. Restraint Order;
b. Confiscation Order;
c. Variation;
d. Management Receiver Order;
e. Enforcement Receiver Order;
f. Contempt of Court.

1.11 Output Production (CO)

Reference ID	Requirement
APPS/R/OPROD/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CO (18.00) CMS FS Cases subsystem

1.12 Output Production (WCO)

Reference ID	Requirement
APPS/R/OPRODW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCO (18.00) WMS FS Cases subsystem

Background / Scope: The Output Production sub-section of the Cases subsystem includes the functionality which generates outputs from case-related information and progresses those outputs which are sent electronically.

The concept of ‘document packs’ is fundamental to the CMS and WMS approach to output production. Document Packs are logically grouped documents associated with a specific User production task. The User may select one or many of the documents in the pack for production.

Output documents and document packs may be requested in four ways:

- The User makes ‘ad hoc’ document pack requests directly from the Communications tab (CG08S) of ‘CG01S: Case Details’. No User task is associated with these requests.
- The User makes non ad hoc requests via other screens (e.g. the Witnesses tab (CG04S)). Non ad hoc requests may result in a task being raised to ensure that the User follows through specification of the pack contents and sends these.

- CMS may itself create a task to prompt the User to produce and send a pack. The pack will be linked to the system generated task. Appendix G categorises each pack and the relationship the pack has with tasks.
- When a single document is being created for immediate dispatch, some screens offer a shortcut facility. CMS creates a document pack and generates the document immediately in MS Word. When the document is completed, CMS automatically marks the document and pack as dispatched.

Functionality in this sub-section is used to manage these specifications and to ensure that document/pack production tasks are marked as complete when appropriate.

1.13 Output Generation

Reference ID	Requirement
APPS/R/OGEN/001	The Supplier shall ensure that the template and the fields contained therein remain unchanged except via the Change Control Procedure once Approved by the Customer The standard template and fields are set in the functional specifications: • 453001_G (18.00) CMS FS Generated Outputs • 453001_G (18.00) WMS FS Generated Outputs

Background / Scope: The standard outputs are generated by populating a number of fields from the data base. For example, An MS Word template exists for each letter to be generated by the system. Angled brackets are used in the template to denote automatically-populated output fields. The system replaces the output field in the letter template, including its angled brackets, with the corresponding data item(s) derived from the database using a defined set of rules.

1.14 Print View

Reference ID	Requirement
APPS/R/PRINT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_H (18.00) CMS FS Print Views • 453001_H (18.00) WMS FS Print Views

Background / Scope: Print views allow the content of the some of the screens within CMS to be produced in a 'print-friendly' format, as well as providing views for specific types of information that has been recorded against the case.

In general, print views are invoked from the print menu in the CMS menu bar, although there are some instances where they are invoked directly from a screen.

When a print view is invoked it will print a report using details retrieved from the case in context, for example the case displayed in the case details screen at the point when the 'Print Current' options is selected.

1.15 Hearing Preparation (CP)

Reference ID	Requirement
APPS/R/HEARP/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CP (18.00) CMS FS Cases subsystem

Background / Scope: The Hearing Preparation sub-section of the Cases subsystem includes the functionality needed to progress a case to the point where it is ready for its next hearing. When the date of the next hearing for a case is set (either at registration or when a hearing outcome is recorded which schedules the next hearing) the Control Subsystem will raise an event which may cause this sub-section to raise tasks preparation for that hearing. That task will navigate to the Prepare Panel. This panel contains facilities for recording:

a. An outline of the allegations made in the charges or indictment;
b. Any issues which the preparing lawyer or caseworker has identified that may be encountered during the hearing (which may be driven by comments made by the reviewing lawyer);
c. Any aggravating features relevant to the case which the prosecutor should present in court;
d. A short analysis of the case aimed at the court prosecutor;
e. Notes for inclusion in the section 41 schedule (e.g. related offence listed on the indictment).
f. Enclosures for the brief.
g. Actions to be carried out in preparation for the hearing.

1.16 Case Review (CR)

Reference ID	Requirement
APPS/R/CREV/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CR (18.00) CMS FS Cases subsystem

Background / Scope: The Case Review section of the Cases subsystem supports the review of Cases registered on CMS. It provides facilities for recording annotations of reviews made either in court or in the office, and for recording decisions that the reviewing lawyer takes

such as suitability for prosecution based on public interest and sufficient evidence considerations. CMS will use tasks to ensure that lawyers are aware which cases have not yet been reviewed and that review outcomes are recorded.

1.17 Case Transfer (CT)

Reference ID	Requirement
APPS/R/CTRAN/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CT (18.00) CMS FS Cases subsystem

Background / Scope: When a case is registered within CMS that case will be associated with the Operational Unit which registers the case. This association governs, at Operational Unit level, responsibility for the prosecution of that case. Within the Operational Unit prosecutors and caseworkers will be allocated to the Case using the facilities described in the Case Allocation (CA) sub-system.

Frequently Cases will need to be transferred from Operational Unit to another. This will commonly be from a (criminal justice) Operational Unit to a related (Trial) Operational Unit when a case is found not suitable for summary trial or at committal, but could be between any Operational Unit or Business Unit. The majority of case transfers will follow the outcome of a Hearing, but in a small number of situations a Case may be transferred without a Hearing taking place. It will occasionally be necessary to transfer large numbers of cases as a result of organisational changes within the Customer or, potentially, partners in the Criminal Justice System.

CMS shall support the transfer of cases between Customer Operational Units, and this will include transfers between Units in different Customer Business Areas. A transfer will be instigated by a User who will navigate to screen ‘CT01S: Transfer Case’. This screen shall list one or more cases selected by the User for transfer and allow the User to specify for each case which Operational Unit that case should be transferred to.

1.18 Case Transfer (WCT)

Reference ID	Requirement
APPS/R/CTRANW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCT (18.00) WMS FS Cases subsystem

Background / Scope: When a case is registered within CMS, it will be associated with a Witness Care Unit (WCU), this being either one selected by the User on registration or, if none is specified then the default Witness Care Unit for the Case. Once the WCU has been set for the Case during registration, then it cannot be changed in CMS. However a WMS User with the 'Transfer Case' Designated Access Right may change the WCU manually within WMS using the Transfer Case facility. WMS shall support the transfer of cases between Witness Care Units, and this will include transfers between Operational Units in the same, or potentially different Customer Business Areas.

1.19 Victim Code Communications (VC)

Reference ID	Requirement
APPS/R/VCC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_VC (18.00) CMS FS Cases subsystem

Background / Scope: The Victim Code Communications section of the Cases subsystem details the screens used to record details of Victim Code communications on a particular Case. These screens allow the User to add, edit, and delete records of the Victim Code Communications, as well as providing a summary of the Victim Code Communications made and indicating whether or not the Victims are identified as vulnerable or intimidated. Some Victim Code requirements have shorter target timescales for communicating with vulnerable or intimidated victims.

The data captured is used by MIS to report on the Customer's compliance with the Victim Code requirements.

1.20 WMS Victim Code Functionality (WVC)

Reference ID	Requirement
APPS/R/WVC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WVC (18.00) WMS FS Cases subsystem

Background / Scope: The Victim Code places statutory obligations on Witness Care Units to:

- Complete a full needs assessment for all victims where a not guilty plea is entered.
- To communicate various events in the progress of a case to the victim(s) associated with that case within specified timescales.

These screens allow the User to add, edit, and delete records of these Victim Code Communications, as well as providing a summary of the Victim Code Communications made and indicating whether or not the victims are identified as vulnerable or intimidated. Some

Victim Code requirements have shorter target timescales for communicating with vulnerable or intimidated victims.

1.21 Hearings Subsystem (H) - CMS

Reference ID	Requirement
APPS/R/HCMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_09 (18.00) CMS FS Hearings Subsystem

Background / Scope: The Hearings (H) subsystem is responsible for the capture of information related to hearings in the CMS. A number of screens, functions and rule sets are included. These support all of the types of hearing, which can take place throughout the life of a case, whether they are in Magistrates Court or Crown Court. The screens, which are provided, are designed to be re-used for each type of hearing that can take place. These screens support recording of hearings and the recording and updating of hearing outcome information.

In addition to recording hearing & hearing outcome information, this subsystem is responsible for initiating actions, which result from a hearing. This is achieved using rule sets, which invoke tasks. Actions over and above these tasks include the splitting and merging of cases.

Functionality in this subsystem is invoked by events raised in the Monitoring subsystem and navigation events created by the User. Once record hearing functionality is complete, an event is raised to initiate further actions in the CMS.

1.22 Hearings Subsystem (H) - WMS

Reference ID	Requirement
APPS/R/HWMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_09 (18.00) WMS FS Hearings Subsystem

Background / Scope: The Hearings (H) subsystem captures Case information related to hearings in the WMS. A number of screens, functions and rule sets are included. These support all of the types of hearing, which can take place throughout the life of a case, whether they are in Magistrates Court or Crown Court. The screens are designed to be re-used for each type of hearing that can take place.

These screens support:

a. ensuring that all called witnesses have been warned prior to a trial hearing;
b. viewing case progress and history at a glance;
c. recording and reviewing Sentence and Bail notes;
d. recording Witness attendance at hearings.

In addition a WMS task model will be provided to prompt WMS Users to perform key activities.

1.23 Materials (M)

Reference ID	Requirement
APPS/R/MAT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MR (18.00) CMS FS Material Subsystem

Background / Scope: The Material Subsystem is responsible for capturing all Case Material received by the Customer throughout the life of a case. This includes the capture of initial information when a case is registered, and the capture of all other information related to a case.

The Material Subsystem supports both the manual entry, and electronic receipt of case material. The term 'Case Material' is quite encompassing. In this case, it includes the following types of information:

a. Information entered by a User via screens.
b. Documents attached to a Case by Users. This could include standard forms containing case information or ad hoc correspondence.
c. Structured information received electronically through the CMS external interface.
d. Unstructured documents received through the CMS external interface. Again, this could include standard forms or ad hoc correspondence.

The material subsystem is responsible for capture, storage and management of each of these types of information as they are received throughout the life cycle of a case.

1.24 Electronic Receipt of Unstructured Material (MU)

Reference ID	Requirement
APPS/R/UNSTRUMU/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MU (18.00) CMS FS Material Subsystem

Background / Scope: The Electronic Receipt of Unstructured Material subsection contains functionality for handling:

a. Unstructured material (i.e. electronic documents) that are received through the CMS external interface;
b. A minimal set of structured data that has been obtained from parsing documents received through the external interface;
c. The addition of material to existing cases manually using a CMS screen.

1.25 Electronic Receipt of Structured Material (ME)

Reference ID	Requirement
APPS/R/UNSTRUME/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_ME (18.00) CMS FS Material Subsystem

Background / Scope: The Electronic Receipt of Structured Material sub-section of the Material subsystem is responsible for the functionality relating to the handling of structured case data that is received electronically from the CMS external interfaces.

The subsystem is triggered by the Support system after it has received a message and broken it down into logical messages. It supplies this subsystem with a pending message representing the logical message which carries the structured data from the logical message, and is linked to a document if the logical message included one.

1.26 Electronic Receipt of Structured Material (MP)

Reference ID	Requirement
APPS/R/STRUMP/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MP (18.00) CMS FS Material Subsystem

Background / Scope: The Electronic Receipt of Structured Material subsystem is responsible for the functionality relating to the handling of structured case data that is received electronically from the CMS external interface. The subsystem handles the receipt of messages, validates the contents of the messages against rules and if all validation passes, stores the information for use on case progression related screens. The subsystem also creates and sends messages as a result of a User action.

1.27 CMS Material Archiving (MA)

Reference ID	Requirement
APPS/R/CMSMA/001	The Supplier shall implement archiving functionality for records in line with the Customer Archiving Policy. The following strategy will be implemented for Case Material in the CMS: a. Three months after a case is concluded (finalised or discontinued), the case will be flagged as archived, unless it has already been marked as of long-term interest. At this point, the CMS will set a retention period for the case. The period will depend on the type of the case, as specified in the Records Management Manual in the Bibliography. b. The Case Material for all archived cases will be retained on-line and Users will be able to search for and access Case Material for archived cases by specifying a flag in the search criteria. Users will be able to search for 'live' cases (the default), or 'archived' cases, or both. c. The CMS will monitor the retention periods for all archived cases and when a retention period expires the CMS will provide facilities to destroy the case by removing all data and documents from the system and will write a case destruction record to the ERMS. When a case is marked as of long-term interest, it will be retained in the CMS database and will not be flagged as archived. The CMS will transfer ownership of these cases to the Customers Records Management Unit three months after the conclusion of the case. d. The CMS will provide facilities for Users to forward cases to the Customer Records Management Unit where the allocated lawyer thinks there should be a review before the case is destroyed, or for cases that are subject to a preservation order under section 17(2) of the Criminal Appeal Act 1995. The Customer Records Management Unit Users will use the CMS to manage, review and when appropriate destroy these cases.
APPS/R/CMSMA/002	For information: the detailed functional specification is set out within the document titled "453001_07_MA (18.00) CMS FS Material Subsystem".

Background / Scope: The Archiving functionality within the Material subsystem is responsible for handling those activities post finalisation which are involved in archiving finalised cases and retrieving them from storage with the Customer's ERMS supplier when necessary.

1.28 User Interface Requirements

Reference ID	Requirement
APPS/R/UIR/001	The Supplier shall deliver the functionality as set out in the detailed

Reference ID	Requirement
	functional specifications: • 453001_14 (18.00) CMS FS User Interface Requirements • The Style Guide is set out at 453001_D (18.00) CMS FS User Interface Style Guide

Background / Scope: The requirements described here are generic and applicable to the system as a whole and are not intended to describe User interaction with any specific screen.

The Style Guide specifies the look and feel of each type of control used on screen as well as layout and behaviour general to every screen. The guiding principles are as follows:

a. The system will be easy to use by Customer staff
b. The CMS will be modern and User-friendly
c. The system will employ a User Interface which is consistent for all Users across the Customer

Users will input data into the system by the use of:

a. Drop down list. Users will be able to select a single data value from a list of pre-defined values.
b. Radio buttons. These will be used where it is appropriate that the User selects only a single data value from a choice of pre-determined values.
c. Check boxes. These will be used where the User can select a single or multiple data values from a choice of pre-determined values.
d. Free text. Free text fields will allow Users to enter comments and other data that cannot be entered using one of the above methods. Users will be able to copy text from a screen and paste from the windows clipboard.
   Any highlights, annotations or other modification to documents will be made and viewed using functions of MS Word.

1.29 Control (L)

Reference ID	Requirement
APPS/R/CONTL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_05 (18.00) CMS FS Control subsystem

1.30 Control (WL)

Reference ID	Requirement
APPS/R/CONTW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications:

Reference ID	Requirement
	• 453001_05 (18.00) WMS FS Control subsystem

Background / Scope: The Control Subsystem links the other CMS subsystems into a coherent system. It defines elements of the User interface which provide access to the system such as menus and the login screen.

Tasks, which provide the mechanism by which the system informs its Users of actions which they need to complete, are specified in this subsystem including background handling and the screens by which Users can view and manage tasks.

This subsystem also defines the controlling rule sets which join together the processes and functions from this and other subsystems. These rule sets collectively manage the lifecycle of each case.

1.31 Monitor (T)

Reference ID	Requirement
APPS/R/MONT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_06 (18.00) CMS FS Monitor Subsystem

1.32 Monitor (WT)

Reference ID	Requirement
APPS/R/MONWT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_06 (18.00) WMS FS Monitor Subsystem

Background / Scope: The Monitor Subsystem is responsible for handling all time-related activities performed by the CMS application. This includes: the escalation of incomplete tasks, the generation of time-triggered tasks, and periodic system behaviour such as case destruction.

Note that the Monitor Subsystem does not interact with any other sub-systems directly, and the diagrams provided in the functional specification only illustrates the subsystem's interaction with time.

1.33 Report (R) – CMS

Reference ID	Requirement
APPS/R/RCMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_10 (18.00) CMS FS Report Subsystem
APPS/R/RCMS/002	The Supplier shall ensure that all standard MIS reports can be run, without the Customer having to request any special access to data
APPS/R/RCMS/003	The Supplier shall when requested, run ad-hoc SQL reports

Background / Scope: The Report subsystem is responsible for generating all non-Management Information System (MIS) reports. Non-MIS reports are operational reports required by a Customer Business Area or Operational Unit or Customer headquarters for the day-to-day management of live cases. This subsystem is not responsible for generating reports on Customer performance indicators or Customer Performance Monitors.

The system supports the following reports:

a. **Police Unit Case Allocation Report**: lists all cases owned by an Operational Unit with details of the allocated and re-allocated lead prosecutor and lead case worker in the period specified by the User. The report is intended to be passed to the police stations which the Operational Unit deals with to inform the police which lawyers and caseworkers are responsible for each case.

b. **Cases for Hearing Report**: lists cases which have a hearing at a specified court scheduled in the period specified by the User.

c. **Outstanding Upgrade Review Check Report**: lists cases within an Operational Unit for which a upgrade file has been received but not reviewed within fourteen days of receipt.

d. **Hearing Outcome Check Report**: lists cases within an Operational Unit for which a hearing has taken place but no outcome recorded and the hearing was more than seven days ago.

e. **Appeal Date Check Report**: lists appeal cases within an Operational Unit which have not had a hearing date recorded within fourteen days of registration.

f. **Case Directions Report**: lists the total number of outstanding and complied directions associated with cases in an Operational Unit that have a hearing in the specified date range with a next hearing at a specified court. The case directions are further broken down in terms of the due date and compliance date of the directions.

g. **Cases with Custody Time Limits Report**: lists all cases within a unit which have an active CTL. The report includes the earliest CTL expiry date for each case and the next

hearing date. A date range, in which the reported CTLs expire, may optionally be specified.

h. **RMU On Loan Cases Report**: lists all cases owned by the RMU which are marked as on-loan to another Operational Unit.

i. **Case Monitoring Report**: lists cases which have a specified monitoring code set, or a specified type of defendant, or have an identified victim.

j. **Stock-take Report**: lists all active cases owned by an Operational Unit for the purpose of performing a stock-take within that Operational Unit.

k. **Ongoing Pre-Charge Cases** either lists 'Inactive Cases' that have a latest pre-charge decision occurring more than a specified number of weeks in the past (up to a maximum of 52 weeks), or lists 'Follow Up Date Cases' with a follow-up date within a date range. It can also be used to identify cases with incomplete consultations i.e. where either no consultation has been started or the latest consultation has not been marked as complete.

l. **Out of Area Audit** lists the number of out of area searches performed by each User in a specified Operational Unit and date range.

m. **Crown Court Cases with No Counts** lists all live charge cases in an Operational Unit which have offences marked as 'In Crown Court' but do not have any counts created on the system.

n. **Unsuccessful Outcome** lists all finalised cases in an Operational Unit which have either a chosen adverse outcome, all adverse outcomes or where costs have been set against the Customer.

o. **Serve Case Date** lists all live charge cases in an Operational Unit which have a serve case date specified within the date range.

p. **Outstanding Warrants** lists all the defendants that are Admin Finalised and have a last hearing with an outcome of WWB or WNB recorded within the date range.

q. **Outstanding Victim Code Comms Report** lists victim code communications records associated with cases in the selected Operational Unit that are outstanding or due to be by a specific date.

r. **Confiscation Cases** lists all orders, i.e. Restraint, Confiscation, Variation, Management Receiver, Enforcement, Contempt of Court, whose Order Lodged or Order Granted / Refused falls on or within the Report Start and Report End dates for the selected Operational Unit.

s. **Outstanding Asset Recovery Reminders** lists all incomplete asset recovery reminders that fall within the Report Start and Report End dates for the selected Operational Unit or area.

t. **Asset Recovery Hearings.** This is used to identify those asset recovery related hearings (as entered on the Manage Orders screen) that are scheduled to occur within the report date range.

u. Receiver Orders - Discharged lists all enforcement or management receiver orders that have been discharged and the associated cases in a User specified month

v. No longer available as a specific Report format

w. Asset Recovery Review Cases lists all those cases which have been given a File Disposal of 'Review', whose Review date is within the reporting period and is expected to be returned from a 3rd party storage site for review. This report is visible in CMS only.

x. Archived Cases list the references of only those boxes containing the File Jacket. Special Casework Division staff can then use the Archive Cases screen to identify other boxes relating to this case.

y. Archive Activities allows the User to print out a list of boxes for which the following activities were carried out on the specified day Box Reference was generated Box status was updated from Recalled to Stored or vice versa..

z. Reactivated Cases allows the User to identify case reactivations that have caused or will cause additional PI credits in MIS on finalisation.

aa. Threshold Test Cases lists those suspects/defendants in cases within a specified Operational Unit which have been charged under a Threshold Test and have not been subject to a Full Code Test.

bb. PCD Charge Discrepancy lists all cases where the 'Check Unauthorised Charge(s)' task has been raised, where the status of the task matches the search criteria.

cc. Restraint and Confiscation Cases lists cases and any Restraint Orders where active cases have a 'Restraint and Confiscation' proceeding type within a specified unit where the cases are allocated to any or a specified prosecutor and / or caseworker.

dd. Enforcement Cases lists active cases and any Confiscation orders with an 'Enforcement' or 'Enforcement (for uplift)' proceeding type within a specified unit where the cases are allocated to any or a specified prosecutor and / or caseworker.

ee. Restraint and Confiscation - Assurance lists active cases and any Restraint Orders where cases have a 'Restraint and Confiscation' proceeding type within a specified unit. Note: this report contains a different set of information to the 'Restraint and Confiscation Cases' report.

ff. Enforcement - Assurance lists active cases and any Confiscation Orders where cases have a 'Enforcement' or 'Enforcement (for uplift)' proceeding type within a specified unit. Note: this report contains a different set of information to the 'Enforcement Cases' report.

gg. Enforcement Receivers lists non-discharged Enforcement Receiver Orders that are granted and/or to which a receiver has been appointed on active cases that have a 'Restraint and Confiscation', 'Enforcement', 'Enforcement (for uplift)', 'Civil Litigation' or 'Civil Recovery' proceeding type within a specified unit.

hh. Management Receivers lists non-discharged Management Receiver Orders that are granted and/or to which a receiver has been appointed on active POC cases within a specified unit.

Note: cc to hh above relate to Proceeds of Crime Cases only and are only available in the Customer's central casework units (i.e. only available to User's with Designated Access Rights).

1.34 Report (WR) – WMS

Reference ID	Requirement
APPS/R/RWMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_10 (18.00) WMS FS Report Subsystem

Background / Scope: The Report subsystem is responsible for generating all operational reports, that is reports generated from case data in the CMS/WMS database. This subsystem is not responsible for generating reports on performance indicators.

The system supports the following reports:

WAVES Report: lists, for a given Customer Business Area, the contact details for a sample of victims and witnesses which are suitable for inclusion in the quarterly Witness' and Victims' Experience Survey (WAVES). The report is delivered to the survey company via the Home Office (outside of the scope of this system).

Outstanding Victim Code Comms Report; This report will show WMS victim code communications records associated with cases in the selected Operational Units. It will list communications of specified types.

WMS Case Monitoring Report; Lists all cases that have a specified monitoring code selected and a hearing start date within the given report start and end date. The report will list Defendants, Hearing information and Customer staff allocated to the case.

1.35 Configuration (F)

Reference ID	Requirement
APPS/R/CONF/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_11 (18.00) CMS FS Configuration Subsystem

Background / Scope: The Configuration subsystem provides the functionality to allow the User to interact with the configuration data. This includes:

a. Maintenance of static data.
b. Maintaining localised views of static data.
c. Maintenance of User information.

The Configuration subsystem breaks down into the following subsections:

I. Static Data (FD). This subsection is responsible for the maintenance of static data. It provides the functionality to add, edit and disable static data.
II. Security (FS). This subsection is responsible for the maintenance of User information and the management of CMS security.

1.36 Configuration (WF)

Reference ID	Requirement
APPS/R/CONWF/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_11 (18.00) WMS FS Configuration Subsystem

Background / Scope: The Configuration subsystem provides the functionality to allow the User to interact with the configuration data. This includes:

a. Maintenance of User information;

b. Maintaining localised views of static data.

The configuration subsystem breaks down into the following subsections:

a. Static Data (WFD). This subsection is responsible for the maintenance of static data. It provides the functionality to add, edit and disable static data.
b. Security (WFS). This subsection is responsible for the maintenance of User information and the management of WMS security.

1.37 Support (S)

Reference ID	Requirement
APPS/R/SUPPS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_12 (18.00) CMS FS Support Subsystem

Background / Scope: The Support subsystem models system functions that support several other functional areas rather than belonging solely within one subsystem. These functions are generic and do not contain specific business logic. Libraries of utilities will cover the following areas:

a. handling incoming electronic messages;
b. storage in and retrieval from the document store;
c. viewing the audit trail;
d. finding cases;
e. Searching for and browsing case information which has been migrated from legacy case tracking systems.

The Support subsystem is broken down into a number of subsections. These are described below:

a. External Interfaces (SI) – This functional area defines the external interfaces of the CMS. It provides generic functions that handle the receipt of electronic Case Material from the police or other sources, and the transmission of electronic reports or requests for information to the police. It is responsible for the receipt, validation and storage of data and documents received via each electronic interface type. It is responsible for message error handling and auditing the receipt of electronic messages. It is also responsible for providing links to legal reference material available via various Internet sites.

b. Electronic Document Handling (SD) – This functional area manages the storage, retrieval, copying and deletion of electronic documents within the CMS. It handles documents received from external bodies, documents created by the CMS, documents created by Users which are being attached to cases (this includes documents scanned using desktop software which are attached to a case).

c. Audit Trail (SA) – This functional area provides facilities for system Users to view all auditable events and completed tasks.

d. Find Cases (SF) – This functional area provides facilities to retrieve a case or cases by (1) entering search criteria and (2) scanning the physical case file barcodes. A number of screens in other subsystems can then be accessed to allow work on the found cases.

e. Legacy Cases (SL) – This functional area provides facilities for searching for cases which have been migrated into CMS from legacy case tracking systems. Once found, cases can be browsed for information such as archive location.

1.38 Support (WS)

Reference ID	Requirement
APPS/R/SUPPWS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_12 (18.00) WMS FS Support Subsystem

Background / Scope: The WMS Support subsystem provides functionality to support the following:

a. viewing the audit trail;
b. finding cases.

The Support subsystem is broken down into a number of subsections. These are described below:

a. Audit Trail (WSA) – This functional area provides facilities for system Users to view all auditable events and completed tasks.

b. Find Cases (WSF) – This functional area provides facilities to retrieve a case or cases by (1) entering search criteria and (2) scanning the physical case file barcodes. A number of screens in other subsystems can then be accessed to allow work on the found cases.

1.39 Screen Layout

Reference ID	Requirement

APPS/R/SCREEN/001	There are a number of screens that make up CMS and its sub systems.
	The Supplier shall ensure these screens remain unchanged except via change control and once agreed with the Customer.
	
	The screen layouts are further detailed in the following documents:
	a. 453001_B (18.00) CMS FS Configuration Subsystem Screen Layout;
	b. 453001_B (18.00) CMS FS Control Subsystem Screen Layout;
	c. 453001_B (18.00) CMS FS Hearings Subsystem Screen Layout;
	d. 453001_B (18.00) CMS FS Material Subsystem Screen Layout;
	e. 453001_B (18.00) CMS FS Report Subsystem Screen Layout;
	f. 453001_B (18.00) CMS FS Support Subsystem Screen Layout;
	g. 453001_B(W) (18.00) WMS FS Case Subsystem Screen Layout;
	h. 453001_B(W) (18.00) WMS FS Control Subsystem Screen Layout;
	i. 453001_B(W) (18.00) WMS FS Hearings Subsystem Screen Layout;
	j. 453001_B(W) (18.00) WMS FS Report Subsystem Screen Layout;
	k. 453001_B(W) (18.00) WMS FS Support Subsystem Screen Layout;
	l. 453001_B (18.00) CMS FS Case Subsystem Screen Layout;
	m. 453001_B(W) (18.00) WMS FS Material Subsystem Screen Layout;
	n. CD121_453001_B(W) (18.00) WMS FS Configuration Subsystem Screen Layout.

1.40 Logical Data Model

Reference ID	Requirement
APPS/R/LDM/001	The Supplier shall ensure that the logical data model and all entities and attributes contained therein remain unchanged except via change control and once agreed with the Customer. The logical data model is detailed within the document titled "453001_C (18.00) CMS FS Logical Data Model"

Background / Scope: There are a number of logical data attributes that make up CMS and its sub systems.

1.41 Management Information System (MIS)

Reference ID	Requirement
APPS/R/MIS/001	The Supplier shall ensure that the MIS described therein remains unchanged except via change control and once agreed with the CUSTOMER. The SUPPLIER shall deliver the functionality as set out in the following documents: • 553001 (13.00) MIS Functional Specification • 553001 (13.00) MIS Functional Specification - Appendices

Background / Scope: As a partner application for the CMS a Management Information System (MIS) has been produced to allow high level reporting against the data collected by the CMS.

The MIS is a database, separate from the CMS, which stores case information extracted on a nightly basis from the CMS. The extraction process anonymises data in the sense that personal information is not extracted, e.g. for a defendant, gender and ethnicity will be extracted but not name and address details.

The Management information System functional specification lists each object in the specified universe, together with the following information:

a. the name of the object, as it will appear to the User in the universe;
b. the type of object, either a dimension (D) or measure (M). A measure is a tally, or total count. A dimension is a condition on a measure;
c. the class into which the object has been organised.

1.42 Reporting

Reference ID	Requirement

Reference ID	Requirement
APPS/R/REP/001	The Supplier shall ensure that the reporting described therein remains unchanged except via change control and once agreed with the Customer. The Supplier shall deliver the functionality as set out in: • 553001 (13.00) MIS Functional Specification – Reports

Background / Scope: There is a "public folders" folder, which contains a set of reference reports that are accessible by all Users with Designated Access Rights for MIS.

1.43 WMS Manual Entry

Reference ID	Requirement
APPS/R/WMSM/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07 (18.00) WMS FS Material Subsystem

Background / Scope: The WMS Add Communications screen enables WMS Users to add documents to cases. Documents are files that can be opened in MS Word.

1.44 CMS External Interface requirements

Reference ID	Requirement
APPS/R/CMSX/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 25501706 (1.00) Police XML Interface Business Process Document

Background / Scope: The interfaces were initiated to meet a demand from the police, the Magistrates' Court (MC), and other organisations for the electronic exchange of structured case information. The primary aim of an interface is to reduce the amount of information that would otherwise need to be re-keyed into the CMS.

Electronic interface for structured communication with CJO systems and others including:

a) Police, (local and national forces);

b) Courts, Crown and magistrates' courts;

1.45 Police Interface – Version 2

Reference ID	Requirement
APPS/R/POL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 50403021 (1.2) Two-Way Police XML Interface Business Process Document

Background / Scope: The initial model interface simplified business processes to a series of simple messages in order that messages could be sent from Police forces to the Customer (a 'one-way' system). By using a series of such simple messages, it is practical to construct larger messages that mimic *the current paper transactions within the business processes*

The second version of the interface implemented a two-way messaging system involving the Case Management System (CMS) and associated Witness Management System (WMS) which share a common database and a range of systems in place with local Police forces including the National Strategy for Police Information Systems (NSPIS) Custody and Case Preparation products, Niche RMS and a range of local Police force systems. The interface is standardised, but can be used in various ways to support local working practices.

The 1st version of the interface continues to be supported, thereby allowing Police forces flexibility in their implementation of changes.

1.46 Courts Interface

Reference ID	Requirement
APPS/R/COURTI/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: a. <10705711002 CMS to CCDCS ICD 1.00>; and b. "50404010 CMS API Interface Control Document (2.02)"

Background / Scope: The interface for the Crown Court is to the DCS (Digital Court System aka Caselines) there are two ICDs (Interface Control Documents) that describe this interface:

a. the first is for outbound from CMS to DCS. This document reference is <10705711002 CMS to CCDCS ICD 1.00>. This document is owned by a third party; Netmaster.
b. the second is to the CMS API for inbound from DCS to CMS. This document is titled "50404010 CMS API Interface Control Document (2 02)" and shall be provided.

The interface for the Magistrates court is the interface between CMS and the HMCTS Court Store system, described in document reference <HMCTS Court Store ICD 113.doc> . This document is owned by HMCTS.

Where documents are owned by third parties, such as the HMCTS Court Store above, the Customer undertakes to make the document available during Implementation.

1.47 Interface with Common Platform

Reference ID	Requirement
APPS/R/INTFC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 107 05 72 06 04 CMS to C2I DX Functional Design v1 4

Background / Scope: The CJS Common Platform Programme is designing and delivering a shared process to transform the way practitioners in the Criminal Justice System work. This will benefit everyone who comes into contact with the Criminal Justice System, including judiciary, victims and witnesses, defendants and justice professionals. More information on the CPP can be found at:
https://insidehmcts.blog.gov.uk/2016/06/30/introduction-to-common-platform-programme/

To support the first release of the Common Platform Programme (CPP) case management solution, (C2I), known as Pre-Charge-to-Initial-Details-of-Prosecution-Case (IDPC) a two-way interface between the Crown Prosecution Service's Case Management System (CMS) and the Common Platform is required to facilitate information exchange between the systems.

This interface allows Case Information submitted by Police forces to be received by CMS and to be sent to C2I, and for information prepared on C2I to be returned to CMS.

Once C2I is operational, CMS will continue to receive cases from the Police. Electronic requests for a pre-charge decision will be forwarded to C2I, and returned once the pre-charge decision has been made. CMS will ensure that the decision is communicated back to the police. Where a suspect is charged, CMS will also forward the charges to C2I where the IDPC may be produced and made available to the defence using the Defence Portal.

The interface with the Common Platform allows pre-charge decisions, initial witness selections and the preparation for the initial details of the prosecution case (IDPC) to be undertaken on the Common Platform. CMS will continue to progress the case after the pre-charge decision stage has completed, through to its conclusion.

1.48 CMS Interface requirements - Witness Care Community Portal (WCCP)

Reference ID	Requirement
APPS/R/INWCCP/001	As and when reasonably required the Supplier shall hold regular meetings with the other CJO's (Government participants in Criminal Justice Integration Unit (CJIU) or its successor), especially the Police and Courts, to present updates to the corporate standard for Information Management and so facilitate the vision of an electronic and joined-up CJS.
APPS/R/INWCCP/002	The Supplier shall, where agreed, represent the Customer at the appropriate CJIU committees.

1.49 Data Currency

Reference ID	Requirement
APPS/R/DATCUR/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCA (18.00) WMS FS Cases subsystem

2. Evidence Management System (EMS)
2.1 EMS - Data Management
2.1.1 Case Creation

Reference ID	Requirement
APPS/R/EMSCC/001	The following will apply to Section 2 below (i.e., 2.1 to 2.3, inclusive): • The Supplier will provide EMS functionality "as is" at the time of RFP issue. The Supplier and the Customer shall work together as part of Services governance to keep the EMS functionality and Documentation under review. Any resulting changes to EMS shall be subject to the Change Control Procedure.
APPS/R/EMSCC/001A	The Supplier shall ensure that a case management structure is defined within the system. This structure will enable the storage and organisation of Case Material. The structure must be configurable. *Examples of a typical structure are given in the Case Creation business scenario* The exact structure required shall be defined by the Customer business process which is subject to continuous improvement practices.
APPS/R/EMSCC/002	The Supplier shall ensure that the system enables the creation of case structure templates which can be applied on a case by case or Operational Unit basis.
APPS/R/EMSCC/003	The Supplier shall ensure that a case can be created in the system irrespective of whether there is Case Material available to store under that case ('an empty case'). *Simply put, cases many be created and left empty until such time that Case Material becomes available.*

Reference ID	Requirement
APPS/R/EMSCC/004	The Supplier shall ensure that a case can be marked as active or closed.
APPS/R/EMSCC/005	The Supplier shall ensure that the system provides an interface and an API if necessary, that allows the creation of a new empty case.

2.1.2 Data Input

Reference ID	Requirement
APPS/R/EMSDI/001	The Supplier shall ensure that Case Material can be manually added to the system from any portable media storage device which is mountable on Windows XP, Vista, Windows 7 and Windows 8 operating systems.
APPS/R/EMSDI/002	The Supplier shall ensure that Case Material can be manually added to the system from any internal network location which is accessible via Customer devices.
APPS/R/EMSDI/003	The Supplier shall provide for the automatic ingest of Case Material, where the system is able to monitor network locations and upload data to a configured case and destination as appropriate.
APPS/R/EMSDI/004	The Supplier shall ensure that the system provides industry standard software interfaces through which data can be ingested and exported. *Web Services would carry particular merit.*
APPS/R/EMSDI/005	The Supplier shall ensure that Case Material can be added to a case at any stage unless the case is marked as closed.
APPS/R/EMSDI/006	The Supplier shall ensure that the digital file types defined in the system specification are ingested by the system.
APPS/R/EMSDI/007	The Supplier shall ensure that at ingest, the source file can be copied to central storage by the system, with the centrally held case file considered the reference.
APPS/R/EMSDI/008	The Supplier shall ensure that at ingest, the source file can be indexed in its current location, with the source file location considered the reference.
APPS/R/EMSDI/009	The Supplier shall ensure that all available file metadata is captured at the file ingest stage. *This includes general file metadata such as date and file size, and file metadata specific to the file type (where available) such as*

Reference ID	Requirement
	image resolution.
APPS/R/EMSDI/010	The Supplier shall ensure that the system enables the capture of additional metadata against an item or group of items at ingest. *Examples include item reference numbers or category identifiers. A specific example from the Central Fraud Group can be found in the Case Creation business scenario.*
APPS/R/EMSDI/011	The Supplier shall ensure that Case Material in a machine-readable-document format is indexed at ingest by the system.
APPS/R/EMSDI/012	The Supplier shall ensure that Case Material which is in an image representation of text format shall have OCR techniques applied at ingest, with the resulting text being indexed. *This refers specifically to documents which have been scanned and had no OCR layer applied.*

2.2 EMS – Search & Processing
2.2.1 Viewing Case Material

Reference ID	Requirement
APPS/R/EMSSP/001	The Supplier shall ensure that the system presents a User configurable interface. Specifically, the size of viewing panes and presence or absence of tool bars and widgets etc. is customisable.
APPS/R/EMSSP/002	The Supplier shall ensure that Case Material metadata can be viewed without viewing the Case Material itself. In general, it should not be arduous to navigate between cases and categories of case material.
APPS/R/EMSSP/003	The Supplier shall ensure that Microsoft Office, Adobe and Microsoft Windows generated text documents are viewable from within the system User interface, without reliance on native Applications.
APPS/R/EMSSP/004	The Supplier shall ensure that all document formats are viewable from within the system User interface, without reliance on native Applications.
APPS/R/EMSSP/005	The Supplier shall ensure that where emails are viewed it is possible to view any attachment associated with the email
APPS/R/EMSSP/006	The Supplier shall ensure that image files can be viewed from within the system User interface, without the reliance on native Applications.
APPS/R/EMSSP/007	The Supplier shall ensure that video replay is achieved from within

Reference ID	Requirement
	system User interface, without the reliance on native Applications.
APPS/R/EMSSP/008	The Supplier shall ensure that audio replay is achieved from within system User interface, without the reliance on native Applications.
APPS/R/EMSSP/009	The Supplier shall ensure that all Case Material can be downloaded to the User's device, and that Case Material can be replayed, viewed or edited using the native application.
APPS/R/EMSSP/010	The Supplier shall ensure that when viewing lists of case material, the material can be sorted according to the metadata described in APPS/R/EMSDI/009 and APPS/R/EMSDI/010.
APPS/R/EMSSP/011	The Supplier shall ensure that when viewing lists of case material, the list can be manually reordered into any order required by the User.

2.2.2 Search & Retrieve

Reference ID	Requirement
APPS/R/EMSSR/001	The Supplier shall ensure that all case material is capable of search based on the case nomenclature described in APPS/R/EMSCC/001 and APPS/R/EMSCC/004.
APPS/R/EMSSR/002	The Supplier shall ensure that all case material is capable of search based on the metadata descried in APPS/R/EMSDI/009 and APPS/R/EMSDI/010.
APPS/R/EMSSR/003	The Supplier shall ensure that all case material is capable of search according to keywords and phrases. This should include all indexed text under APPS/R/EMSDI/011 and APPS/R/EMSDI/012. This requirement includes the ability to search the bundles created under APPS/R/EMSEBC/001.
APPS/R/EMSSR/004	The Supplier shall ensure that all case material is searchable according to the criteria defined in APPS/R/EMSPCM/015 and APPS/R/EMSPCM/016.

2.2.3 Processing of Case Material

Reference ID	Requirement
APPS/R/EMSPCM/001	The Supplier shall ensure that the system enables multiple Users to work on the same case concurrently.
APPS/R/EMSPCM/002	The Supplier shall ensure that case material can be re-categorised from its categorisation at ingest.
APPS/R/EMSPCM/003	The Supplier shall ensure that relationships can be created between files. The minimum capability shall be the creation of 1:1 relationships between items. Examples include email-attachment and statement-exhibit.
APPS/R/EMSPCM/004	The Supplier shall ensure that Microsoft Office, Open Document Format and all other document file types can be converted to PDF

Reference ID	Requirement
	using the system.
APPS/R/EMSPCM/005	The Supplier shall ensure that PDF documents can be split into component documents or combined into a single document using the system.
APPS/R/EMSPCM/006	The Supplier shall ensure that the page order of a PDF document can be edited using the system.
APPS/R/EMSPCM/007	The Supplier shall ensure that configuration management within the system enables the version tracking of case material which is either edited using the system or undergoes a “check out” and “check in” process.
The Supplier shall ensure that the system can enable the following User driven capability when items are processed to include:	
APPS/R/EMSPCM/008	The redaction of document and image file content.
APPS/R/EMSPCM/009	The redaction of audio and video file content.
APPS/R/EMSPCM/010	The annotation of a file.
APPS/R/EMSPCM/011	The capture of comments or notes against a file.
APPS/R/EMSPCM/012	The highlighting of elements within a document.
APPS/R/EMSPCM/013	The rotation of an image.
APPS/R/EMSPCM/014	The addition of hyperlinks within a PDF document.
APPS/R/EMSPCM/015	The Supplier shall ensure that the tracking of a single item of Case Material and the capture of decision making which supports the Customer business process shall be enabled by the system. Examples of this include marking an item as “reviewed”, “used” or “unused”. The complete Customer business process will be provided at a later stage. The Customer business process is governed by a continuous improvement process and as such this element of the system should be configurable to meet changing requirements as they arise.
APPS/R/EMSPCM/016	The Supplier shall ensure the capture of rationale to support the decision making described in APPS/R/EMSPCM/015.

Reference ID	Requirement

2.3 EMS - Presentation of Case Material

2.3.1 Evidence Bundle Creation

Reference ID	Requirement
APPS/R/EMSEBC/001	The Supplier shall ensure that the system enables the creation of an “evidence bundle”, whereby a selection of case material is compiled into a single PDF document. The Supplier shall ensure that this can be achieved either directly by the system or by interfacing to a third party product to perform the bundling using standard or custom bundling parameter specified by the system. The Supplier shall ensure that the bundle content can either be defined manually, or can be complied according to the decisions recorded under APPS/R/EMSPCM/015. The Supplier shall ensure that the order of documents and pages within the bundle can be defined by the User and that documents and pages are capable of being reordered or removed if necessary. The Supplier shall ensure that the bundle will be paginated according to requirements which shall be presented at a later stage and may be complex. The Supplier shall ensure that a bundle index will be auto generated with hyperlinks to the indexed sections. The Supplier shall ensure that hyperlinks can be added between references in the bundle. The Supplier shall ensure that bundles are able to include any item of case material (with the exclusion of video and audio file types), including any redacted (or otherwise edited) or configuration managed version of a case material item. The Supplier shall ensure that an evidence bundle is accessible from within the system. The Supplier shall ensure that an evidence bundle is compatible with both Windows and Apple Mac operating systems. It should be noted that an evidence bundle can constitute hundreds or in some instances thousands of pages. In addition, the Customer’s formatting and pagination requirements are bespoke.

3. SharePoint

Reference ID	Requirement
APPS/R/SHAREP/001	The Supplier shall provide hosting and support for the Customer's Knowledge and Information Management systems, including SharePoint. Development of the systems may be requested by the Customer via the Change Control Procedure.

Note: For a list of the SharePoint Applications please see the table in Annex 2 of Part A of this Call Off Schedule.

4. Support of servers and data hosted outside the data centres

Reference ID	Requirement
APPS/R/SERVSUP/001	NOT USED.
APPS/R/SERVSUP/002	NOT USED.

5. Active Directory

Reference ID	Requirement
APPS/R/ACTIVD/001	The Supplier shall maintain AD Active Directory for Users. This shall include hosting and managing the Customer Public Key Infrastructure in support of active directory domains and certification services.
APPS/R/ACTIVD/002	As part of its Active Directory management responsibilities, the Supplier shall host and manage distributed domain controllers within Supplier data centres in support of active directory domains and certification services.
APPS/R/ACTIVD/003	The Supplier shall maintain federated Active Directory services and allow connections, rights and access control as needed to the federated AD structure hosted within the Azure platform related to the Customer's Office 365 installation.
APPS/R/ACTIVD/004	The Supplier shall perform Domain Administration duties in relation to the CMS Domain. The "CPS" Domain (cps.gov.uk) is the active directory domain for the Customer office infrastructure and includes staff User accounts, EUD accounts, DHCP, DNS, Microsoft Exchange and other components for use across the entire Customer estate. The "CMS" Domain (cmscps.gov.uk) is used within the current incumbent data centres to host computer accounts for computers

Reference ID	Requirement
	managed by the incumbent including those associated with CMS/WMS

6. BES

Reference ID	Requirement
APPS/R/BES/001	BES Infrastructure and support The Supplier is required to host and maintain a secure approved installation, currently BES12, and all associated accounts providing email, calendar and internet browsing capabilities.

7. Email services

Reference ID	Requirement
APPS/R/EMAIL/001	Email white listing, email header translation, email routing and proxy filtering: The Supplier shall provide white listing and AV scanning services and carry out header translation for transmission to and from PNN domains, and support the provision of scan to email services.
APPS/R/EMAIL/002	Email gateways The Supplier shall host and maintain email gateways suitable for routing and filtering email traffic between the Customer domain, AGO domain, HMCPSI domain and the GSi, CJSM and PNN email domains.

8. Group Policy Objects

Reference ID	Requirement
APPS/R/GROUPP/001	The Supplier shall allocate User accounts to organisational units (OUs) based upon the Customer office at which Users' personal file data and account information are stored.
APPS/R/GROUPP/002	The Supplier shall use OU's to host computer accounts for servers, the various EUD types and administrative User accounts.

Reference ID	Requirement
APPS/R/GROUPP/003	The Supplier shall take over and use the Group Policy Objects (GPOs) on the OUs in order to control the configuration of EUDs and to restrict access to Applications and generally provide a consistent and secure desktop environment.

Background / Scope: Group Policy management for EUDs - User accounts are allocated to organisational units (OUs) based upon the Customer office at which Users' personal file data and account information are stored. Group Policy Objects (GPOs) are used extensively on these OUs in order to control the configuration of EUDs and to restrict access to applications and generally provide a consistent and secure desktop environment.

Group Policy Control - User accounts are allocated to organisational units (OUs) based upon the Customer office at which Users' personal file data and account information are stored. Further organisational units exist to host computer accounts for servers, the various EUD types and administrative User accounts.

9. Juniper Remote Access

Reference ID	Requirement
APPS/R/JRA/001	For Remote Access Services (currently a Juniper solution), the Supplier shall provide a secure approved remote access service allowing all Users the ability to connect to central services over the internet utilising both wired and wireless connections.

10. Solidus access

Reference ID	Requirement
APPS/R/SOLI/001	The Supplier shall provide firewalls, terminal services and certificate services in support of the third party Solidus service.

11. Two Factor Authentication System ActivCard

Reference ID	Requirement
APPS/R/2FACT/001	The Supplier shall host and maintain services in support of two factor authentication for both remote access services for Customer Users and remote access services for Police Users accessing WMS.

A.3 Business Critical Systems- Non Functional Requirements

1. General

Reference ID	Requirement
APPS/R/GENNFUN/001	Subject to APPS/R/AVAMAN/003 the Supplier shall make the Systems available for use at all times unless the Systems have to be shut down for planned maintenance or upgrade. In particular the Supplier shall agree communications with the relevant Customer Representative in respect of: (i) notifying Users of any planned withdrawal of service and (ii) providing Users with regular reminders of all planned withdrawals of service.
APPS/R/GENNFUN/002	Subject to APPS/R/AVAMAN/003, the Supplier shall keep outages agreed to withdraw Services, to a minimum. All outages shall be agreed via operational change and shall be confined to the outage window as agreed by the Change Advisory Board.
APPS/R/GENNFUN/003	The Supplier shall ensure that the Services continue to be of sufficient capacity to meet the Customer's operational needs. This includes providing sufficient capacity to cater for growth in use over the Call Off Contract Period.
APPS/R/GENNFUN/004	The Supplier shall enable the Customer to respond to urgent requirements for change in the CJS by providing a fast-track mechanism for amending and enhancing the functionality of the CMS. Such mechanism to be agreed during Implementation.
APPS/R/GENNFUN/005	The Supplier shall provide database backup and operating system updates
APPS/R/GENNFUN/006	The Supplier shall where possible, use remote management techniques to ensure that fixes to problems can be applied without needing engineers to physically attend site.
APPS/R/GENNFUN/007	The Supplier shall provide the flexibility to "fast track" certain changes, where urgent requirements for change have been identified by the Customer. Call Off Schedule 14 (Change Control Procedure) articulates the process for handling such Change.
APPS/R/GENNFUN/008	The Supplier shall ensure that, where possible without detriment to the effective and efficient prosecution of cases, COTS products provided in support of case management are suitable for wider application across the Customer.
APPS/R/GENNFUN/009	The Supplier shall make all information exchange agreements and interface specifications freely available for use by Related Suppliers and organisations without charge. The Customer shall be responsible for putting in place any confidentiality arrangements in place with such Related Suppliers and organisations, as needed.
APPS/R/GENNFUN/009A	Subject to APPS/R/AVAMAN/003, the Supplier shall design the Business Critical Systems solution to be highly resilient to make the Services available to the Customer 24 hours a day, 7 days a week

Reference ID	Requirement
APPS/R/GENNFUN/010	The Supplier shall allow access to the CMS and WMS to non-Customer users on the authority of the Customer.
APPS/R/GENNFUN/011	The Supplier shall ensure that it is possible to control access to case files held on the Case Management System and to fields within a case file to a specific User or group of Users.
APPS/R/GENNFUN/012	The Case Management System shall enable an organisational or functional unit of the Customer to choose whether or not to hold electronic case files or only summary details of some or all of its cases.
APPS/R/GENNFUN/013	The Supplier shall ensure that it is always possible to print all or part of an electronic case file and the summary details of a case as a report.
APPS/R/GENNFUN/014	The Supplier shall ensure that the Case Management System is capable of accepting, storing, processing and reporting on financial data in both pounds sterling and euros.
APPS/R/GENNFUN/015	The Supplier shall perform the necessary administration tasks in support of the Case Management System to ensure that the CMS continues to function efficiently. This shall include database administration activities, backup and archiving activities, restore, system management and network management activities such as general monitoring and health checking.
APPS/R/GENNFUN/016	The Supplier shall ensure the CMS continues to be developed in a modular fashion, to allow changes and enhancements to only impact one or more modules, thus making it easier and less costly to modify the functionality.
APPS/R/GENNFUN/017	For CMS and WMS, the Supplier shall provide and maintain screen options to allow Users to choose to produce correspondence in Welsh and print forms in Welsh or bilingual format. For CMS and WMS, the Supplier shall provide the facilities to enable the Customer to develop and maintain document templates in Welsh and bilingual formats to support this functionality. The Supplier acknowledges that the Services shall be delivered in a manner which is compliant with the Welsh Language Act 1993 and with the Welsh language scheme that the Customer is liable to comply with and where required any change required to ensure such compliance shall be subject to the Change Control Procedure.

Reference ID	Requirement
	The Supplier shall ensure that it is familiar with the Customer's current Welsh language scheme which is available at https://www.cps.gov.uk/cymraeg/assets/uploads/files/CYNLLUN%20IAITH%20GYMRAEG%20-%20WELSH%20LANGUAGE%20SCHEME.pdf.
APPS/R/GENNFUN/018	In consultation with the Customer, the Supplier shall provide a method statement (no more than one page A4) describing how they could deliver the Service under this Call Off Contract to ensure that Users are treated equally whether they require the service in Welsh or English. This method statement shall briefly address: • each key aspect of the service and the anticipated level of Welsh language requirement for this Call Off Contract; • how they will monitor and promote the ability of Users to receive an equal Welsh or English service, and indicate how they would respond to any resulting change in demand for the service to be provided through the medium of Welsh/English.
APPS/R/GENNFUN/019	The Supplier shall deliver the functionality as set out in the detailed functional specifications: "453001_15 (18.00) CMS FS Non-functional Requirements".

Background / Scope: Further non-functional requirements that impact the CMS and WMS applications can be categorised under the following subsections:

a. Security. This section documents the levels of access that can be configured for Cases held in the CMS database. It describes the User roles supported by the CMS and WMS, provides a list of supported access rights and specifies the requirements for auditing. The mechanisms controlling access to a session on the CMS or WMS are described.
b. Availability and Disaster Recovery. This section provides an overview of those aspects of the system design that provide the basis for meeting the system availability and business continuity requirements. The section provides a listing of the availability and disaster recovery requirements that the CMS and WMS shall meet.
c. Volumetrics and Performance. This section provides a summary of the volumetric information that the system will be designed to meet. This section also provides a listing of the performance requirements that the CMS and WMS shall meet.
d. System Management. This section provides a listing of the system requirements such as the frequency of backups etc. that the application and infrastructure design shall support.
e. External Interfaces. This section groups any additional requirements relating to the XML and/or Email Interfaces with the Police. These interfaces interact with the CMS only, but some of the data received by CMS via these mechanisms is also visible in WMS.

2. EMS Non Functional Requirements

2.1EMS – Administrative

2.1.1 User Management

Reference ID	Requirement
	The following will apply to this Section 2.1: • The Supplier will provide EMS non-functionality "as is" at the time of RFP issue. The Supplier and the Customer shall work together as part of Services governance to keep the EMS non-functionality and Documentation under review. Any resulting changes to EMS shall be subject to the Change Control Procedure.
APPS/R/EMSUM/001	The Supplier shall ensure that User roles can be defined in the system to which User accounts can be assigned.
APPS/R/EMSUM/002	The Supplier shall ensure that the permissions and Designated Access Rights can be configured on a per role basis. *This Requirement implies the creation of a tiered User account structure, similar to that described in the roles within the EMS business scenario.*

2.1.2 Access Control

Reference ID	Requirement
APPS/R/EMSAC/001	The Supplier shall ensure that User authentication is performed against Microsoft Active Directory.
APPS/R/EMSAC/002	The Supplier shall ensure that Designate Access Rights to all data and Case Material in the system can be specified and applied to User roles or specific Users, and that .The level of access control granularity is sufficient to define access rights at case and item level.

2.1.3 Management Information

Reference ID	Requirement
APPS/R/EMSMI/001	The Supplier shall ensure that the system provides sufficient administrative information to enable the management of system resources. *In particular, this requirement refers to storage management, User numbers and system hardware utilisation.*

2.1.4 Audit

Reference ID	Requirement
APPS/R/EMSAUD/001	NOT USED.

Reference ID	Requirement
APPS/R/EMSAUD/002	The Supplier shall ensure that the system maintains a record of any User interaction with Case Material where that interaction results in a change to the item or its associated metadata.
APPS/R/EMSAUD/003	The Supplier shall ensure that the system maintains a record of all User management activities described in 2.1.1 User Management above.
APPS/R/EMSAUD/004	The Supplier shall ensure that the system provides audit data to comply with, or facilitate compliance with, the applicable requirements of the baseline control set found in CESG Good Practice Guide 13. This accounting data shall be exported automatically by a standard method such as syslog
APPS/R/EMSAUD/005	The Supplier shall ensure that the system provides audit data to comply with, or facilitate compliance with, the wider requirements of CESG Good Practice Guide 13. In particular the systems shall deliver applicable recordable events and accounting items specified in GPG13 by a standard method such as syslog.

B.1 Non Business Critical Systems of High Importance – Functional Requirements

The requirements set out under this section cover:

#	**System**
1	Boundary Firewalls
2	Checkpoint media server
3	DNS & DHCP
4	EPO Server
5	iChange
6	Interface to iTrent, Zanzibar, HR & e-Learning, CIS, FARMS, ePayFact
7	MBAM Server
8	Print Queue Management
9	Remote Multi Functional Device Management
10	SCCM
11	Server Operating systems (Windows & Unix)
12	SQL

13	Terminal Server
15	Unified Threat Management (UTM)
16	Web Filtering

1. Boundary Firewalls

Reference ID	Requirement
APPS/R/BFIRE/001	The Supplier shall host and support firewalls used on the boundaries of the external interfaces (internet, PSN and Solidus) and internally to maintain the boundary of the Customer and CMS domains and any internal management infrastructure.

2. Checkpoint media server

Reference ID	Requirement
APPS/R/MEDSERV/001	The Supplier shall host and maintain a Checkpoint media server used for providing removable media encryption on selected EUDs

3. DNS & DHCP

Reference ID	Requirement
APPS/R/DNSDHCP/001	DNS, DHCP Management (integrated with AD) The Supplier shall host and maintain internal DNS and external DNS forwarding services and provide DHCP services in accordance with defined IP addressing schema agreed with the Customer

4. EPO Server

Reference ID	Requirement
APPS/R/EPOSERV/001	The Supplier shall host and maintain ePO servers. The Supplier shall maintain on the ePO servers an agreed rule set for the HIPS firewall for EUDs. The Supplier shall maintain up to date AV signatures for EUDs on the ePO servers.

5. iChange

Reference ID	Requirement
APPS/R/ICHANGE/001	The Supplier shall host, maintain and administer the commercial change management workflow system.

6. Interface to iTrent, Zanzibar, HR & e-Learning, CIS, FARMS and ePayFact

Reference ID	Requirement
APPS/R/OTHINT/001	The Supplier shall provide the web connectivity for a range of third party bureau services on the PSN and internet. These shall include, but not be limited to, (interfaces / services related to Basware P2P, iPayview, iTrent, Zanzibar, FARMS, ePayFact, Prosecution Application, College e-Learning portal & Civil Service Learning e-Learning portal, etc.)
APPS/R/OTHINT/002	NOT USED.

Note: For clarity, the definitions of FARMS and ePayFact (referred to above) are as follows:

- **FARMS** (Finance and Resource Management System), is the Customer's payment and accounting system. This is a non-COMPASS contract held by the Supplier on servers in the Bridgend data centre. The Supplier shall provide interface connectivity to this system.
- **ePayFact** is the payroll service used by the Customer.

7. MBAM Server

Reference ID	Requirement
APPS/R/MBAM/001	The Supplier shall host and maintain the central MBAM server used for the management of BitLocker on EUDs.

8. Print Queue Management

Reference ID	Requirement
APPS/R/PRINTQ/001	The Supplier shall host and provide connection to print queues.

9. Remote Multi Functional Device Management

Reference ID	Requirement
APPS/R/MFDEV/001	The Supplier shall host and maintain the environment for Other

Reference ID	Requirement
	Supplier's Print services and provide onward routing into the Customer domain.

10. SCCM

Reference ID	Requirement
APPS/R/SCCM/001	The Supplier shall host and maintain centralised SCCM servers and distribute SCCM packages to servers and EUDs, as requested by the Agency Manager. The Supplier shall complete manual installs of low volume apps on-request in accordance with Call Off Schedule 14 (Change Control Procedure). The Supplier shall carry out non-SCCM based application installations on EUDs in accordance with Call Off Schedule 14 (Change Control Procedure).
APPS/R/SCCM/002	On instruction from the Agency Manager, the Supplier shall update EUD builds via SCCM including the distribution of up to date security patches.
APPS/R/SCCM/003	The Supplier shall create SCCM packages for application distributions to both servers and EUDs. For the avoidance of doubt, the Agency Manager will pass to the Supplier the materials required to create packages for deployment to EUDs and the Agency Manager will test the resulting packages prior to distribution by the Supplier.
APPS/R/SCCM/004	The Supplier shall maintain server builds including the distribution of up to date security patches.
APPS/R/SCCM/005	The Supplier shall maintain terminal server builds including the distribution of up to date security patches.
APPS/R/SCCM/006	NOT USED.

11. Server Operating systems (Windows & Unix)

Reference ID	Requirement
APPS/R/SOS/001	The Supplier shall maintain and security patch all server OSs (Unix and Windows Server). The Supplier shall deploy patches to EUDs via SCCM, on request from the Agency Manager.

12. SQL

Reference ID	Requirement
APPS/R/SQL/001	The Supplier shall host and maintain SQL server instances used in support of miscellaneous Customer applications.
APPS/R/SQL/002	The Supplier shall backup and restore services for the SQL systems used in support of miscellaneous Customer applications.

13. Terminal Server

Reference ID	Requirement
APPS/R/TSERV/001	The Supplier shall provide, maintain and support Terminal services infrastructure / services in the data centres.

Background / Scope: Terminal services infrastructure / services in the data centres and in Customer Premises.

14. Unified Threat Management (UTM)

Reference ID	Requirement
APPS/R/UTM/001	The Supplier shall provide UTM capability for the core firewalls incorporating IDS capabilities.

15. Web Filtering

Reference ID	Requirement
APPS/R/WEBF/001	The Supplier shall provide web filtering including web proxy and white listing services for internet bound traffic.

B.2 Non Business Critical Systems of High Importance – Non Functional Requirements

1. General

Reference ID	Requirement
APPS/R/GNFUN/001	The Supplier shall enable access to all of the Customer's applications or application components hosted at the Supplier's data centres.
APPS/R/GNFUN/002	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall provide second and third line support, including database

Reference ID	Requirement
	backup and operating system updates for the Customer System and applications.
APPS/R/GNFUN/003	The Supplier shall provide a scalable system, so that any growth in Customer capacity requirements can be met, either by increase in server numbers, server processing capability, or data link bandwidth. Any legacy items that cannot be put into the Supplier's Cloud solution for technical reasons will be reviewed on a case by case basis.
APPS/R/GNFUN/004	The Supplier shall ensure server management, including utilities that will enable remote management and monitoring of each server.
APPS/R/GNFUN/005	The Supplier shall record, maintain and monitor all installed software and, except for Transferring In Software, associated licence details. For Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.

C.1 Non Business Critical Systems of Medium Importance – Functional Requirements

The Service Requirements set out in this section cover:

#	System
1	Support for office moves
2	NOT USED.
3	LAN management within the data centres
4	Traffic Management systems
5	Monitoring systems for switches, servers, storage and firewalls

1. Support for office moves

Reference ID	Requirement
APPS/R/SUPMOV/001	The Supplier shall support office moves. The effort for supporting an office move shall be agreed between the Parties under Call Off Schedule 14 (Change Control Procedure).

2. Apple xServe Server

Reference ID	Requirement
APPS/R/APPLE/001	NOT USED.

3. LAN management within the data centres

Reference ID	Requirement
APPS/R/LAN/001	The Supplier shall maintain the LAN environment for all the data centre services (i.e. hosted services at non Customer Premises)

4. Traffic Management systems

Reference ID	Requirement
APPS/R/TRAFF/001	The Supplier will provide, for the Supplier Solution, a suitable bandwidth allowance to the internet. The allowance will be able to burst above this allowance in times of high usage.
APPS/R/TRAFF/002	The Supplier shall provide as part of capacity management both peak and average utilisation of traffic on the internet and PSN links.

5. Monitoring systems for switches, servers, storage and firewalls

Reference ID	Requirement
APPS/R/MONSYS/001	The Supplier shall provide monitoring and health services (currently ACP, WUG and BMC Patrol) for infrastructure services such as switches, servers, storage subsystems and firewalls

C.2 Non Business Critical Systems of Medium Importance – Non Functional Requirements

1. General

Reference ID	Requirement

Reference ID	Requirement
APPS/R/GENMED/001	The Supplier shall enable access to all of the Customer's applications or application components that are hosted at the Supplier's data centres.
APPS/R/GENMED/002	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall provide second and third line support, including database backup and operating system updates for the Customer's applications.
APPS/R/GENMED/003	The Supplier shall also maximise the availability of systems that are not Business Critical Systems.
APPS/R/GENMED/004	The Supplier shall provide the ability for the Customer to increase the hours of availability of the Services, as a permanent or temporary measure. Any such increase will be addressed under Change Control.
APPS/R/GENMED/005	The Supplier shall provide a scalable system, so that any growth in Customer capacity requirements can be met, either by increase in server numbers, server processing capability, or data link bandwidth. Any legacy items that cannot be put into the Supplier's Cloud solution for technical reasons will be reviewed on a case by case basis.
APPS/R/GENMED/006	The Supplier shall ensure server management, including utilities that will enable remote management and monitoring of each server.
APPS/R/GENMED/007	The Supplier shall record, maintain and monitor all installed software and, except for Transferring In Software, associated licence details. For Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.

D General Operational/ Technical Requirements

The requirements set out under this section cover:

#	**System**
1	Supportability
2	Service Performance Reporting
3	License Management
4	Software Asset Management
5	Application Decommissioning
6	Release & Deployment Management
7	Service Validation and Testing
8	Customer Satisfaction
9	Application Development
10	Testing
11	ITA Requirements

1. Supportability

Reference ID	Requirement
APPS/R/SUPP/001	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall ensure that support and maintenance of the hardware and software shall, where reasonably possible, be co-terminus with the Call Off Contract.
APPS/R/SUPP/002	The Supplier Solution shall demonstrate corporate social responsibility by lowering the carbon cost when compared to the current infrastructure for the equivalent capacity.
APPS/R/SUPP/003	The Supplier's supply chain shall demonstrate the use of 'Green IT' throughout the duration of the Call Off Contract.
APPS/R/SUPP/004	The Supplier Solution shall, where practicable, use CE marked components from reputable manufacturers that conform to the appropriate Standards and Regulations specified.
APPS/R/SUPP/005	The Supplier shall ensure that all Components of the hardware and networks shall operate in accordance with their technical specifications.

2. Service Performance Reporting

Reference ID	Requirement
APPS/R/SPR/001	The Supplier shall provide regular and comprehensive Service Performance Monitoring Reports on achievements and trends against Service Levels and on Incidents and issues arising during the previous Service Period. These reports shall provide sufficient information presented in a structured format to enable easy

Reference ID	Requirement
	reconciliation with the Supplier's invoices and shall include, at a minimum, monthly figures (against Service Levels) and trends for: a. Service availability and performance, including hosting platform availability; b. Incident management including details of Incidents Resolved; outstanding Incidents and the steps being taken to effect permanent solutions and fix times for the different Severity Levels of Incidents; c. Processor utilization; d. Alerts during reporting period; e. Capacity and usage reports (monthly and trend analysis); f. where possible, component availability; g. Business Critical Systems Database file growth; The design of the reports, based on the content identified above, shall be agreed by the Parties during Implementation. The Customer shall retain the right to vary the design and content of such reports thereafter and, if there is any impact to the monthly reporting cycle, the Parties shall discuss and agree any adjustments, as applicable. The Customer reserves the right to challenge the information received and the Supplier shall respond to those challenges in a timely manner as directed by the policies, processes and procedures or otherwise.
APPS/R/SPR/002	The Supplier shall produce a Monthly Service Performance Monitoring Report which shall be delivered within 5 Working Days of the Month's end.
APPS/R/SPR/003	The Supplier shall produce a Monthly Finance Report which shall be delivered within 8 Working Days of the Month's end.

3. License Management

Reference ID	Requirement
APPS/R/LICMAN/001	The Supplier shall maintain a clearly defined Software policy, to ensure that when new or additional software purchases are made by the Supplier, checks are made on: • the availability of un-utilised software that has already been purchased; and • the existence of corporate licence or other such agreements or facilities; and • the need for all Software in use to be legitimately licensed.

Reference ID	Requirement
	For Software supplied by the Customer: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.
APPS/R/LICMAN/002	For Software provided by the Supplier, the Supplier shall use a software licencing tool to monitor the number and type of Licenses in use for all such Software utilised to implement the Supplier Solution to deliver the Services ensuring: a. all Software in use is legitimately licensed. The Supplier will notify the Customer of any unlicensed software that is identified and shall delete any such software, when instructed to do so by the Customer. The Supplier shall not be responsible for replacing unlicensed software; b. all Transferring In Software, Supplier Procured Software and Supplier Exclusive Software in use has been Approved by the Customer**.** For Transferring in Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements. For all Transferring In Software, the Supplier shall ensure optimum use is made of all software, both current and legacy, for which licences are held.

4. Software Asset Management

Reference ID	Requirement
APPS/R/SOFTMAN/001	The Supplier shall record all software on the Supplier's CMDB unless otherwise agreed.

Reference ID	Requirement
APPS/R/SOFTMAN/002	As software changes, through either reorganisation, technology refreshment, or because equipment has failed and a replacement has been installed, the Supplier shall record the changes, thus the asset database will be up to date at all times (save to the extent that asset locations have been changed by the Customer without notification to the Supplier).
APPS/R/SOFTMAN/003	The Supplier shall record, maintain and monitor all installed software and associated licence details.
APPS/R/SOFTMAN/004	The Supplier shall provide regular software asset reporting to the Customer. The format and frequency of these reports to be agreed during Implementation.
APPS/R/SOFTMAN/005	NOT USED.

5. Application Decommissioning

Reference ID	Requirement
APPS/R/APPDEC/001	The Supplier shall develop an Application Decommissioning methodology with input from the Related Suppliers, the Agency Manager and the Customer, for the managed removal of an Application from the Customer ICT Environment, including all dependent Interfaces, scripts and Application data.
APPS/R/APPDEC/002	The Supplier shall maintain and update the Application Decommissioning methodology at least annually, providing it to the Customer for review and Approval.
APPS/R/APPDEC/003	The Supplier shall comply with the Approved Application Decommissioning methodology.
APPS/R/APPDEC/004	The Supplier shall ensure that all data records relevant to the Application (including the Service Catalogue) are updated within ten (10) Working Days of completion of the decommissioning Process.

6. Release & Deployment management

Reference ID	Requirement
APPS/R/RELDEP/001	The Supplier shall produce an Apps and Hosting Release Schedule and associated Release Plan(s) and issue these to the Agency Manager and the Customer. The Release Schedule will provide details for at least a three month rolling period.
APPS/R/RELDEP/002	The Supplier shall maintain a record of all software and firmware upgrade and patch updates, updating the records to show when manufacturers issue new versions, which will be reviewed on a regular basis. The Supplier shall make this available to Agency Manager and the Customer on demand.
APPS/R/RELDEP/003	Except as provided otherwise in Call Off Schedule 9 (Software and Assets) the Supplier shall maintain software and firmware versions of all services provided by them as a minimum to vendor recommendation and will action new versions within 4 weeks of being made available or as agreed with the Customer.

7. Service Validation and testing

Reference ID	Requirement
APPS/R/SERVVAL/001	The Supplier shall specify in detail how Releases will be tested and quality-assured.
APPS/R/SERVVAL/002	The Supplier shall submit a release and testing plan for each Release and submit them to an initial assessment by the Agency Manager. The Supplier shall ensure that each Release shall meet stringent Quality Criteria (to be defined and agreed with the Agency Manager).
APPS/R/SERVVAL/003	The Supplier shall conduct release testing and test all release components and all tools and mechanisms required for deployment, migration and back out. The Supplier shall via this process ensure that only components which meet stringent Qquality Criteria are deployed into the live production environment.
APPS/R/SERVVAL/004	The Supplier shall verify with the Agency Manager that conditions (to be defined and agreed with the Agency Manager) are met for the new service to be activated, and to obtain Approval from the Customer that the new service fulfils the agreed Service Level Requirements. In the event that serious Defects are discovered, the actions that should be discharged by each Party shall be decided between the Supplier, Agency manager and Customer.

8. Customer Satisfaction

Reference ID	Requirement
APPS/R/CUSSAT/001	The Supplier shall adhere to and operate in accordance with Complaint Management Policies, Processes and Procedures as directed by the Customer (These will be made available to the Supplier during Implementation). The Supplier shall have agreed procedures for recording and responding to customer complaints and shall ensure that all complaints are reported in Service Management Reports to the Customer.
APPS/R/CUSSAT/002	The Supplier shall assist and co-operate with the Agency Manager in defining and conducting regular Customer satisfaction surveys of the Services they provide and shall have procedures, agreed with the Agency Manager, for responding to any negative output from these surveys.

9. Application Development

Reference ID	Requirement
APPS/R/APPDEV/001	The Supplier Solution shall provide wide support for developer languages and frameworks, where used and required to support CMS/WMS and the Prosecutor App, .including Net framework, ASP.NET, VB.Net, C#.Net, Javascript, JQuery, Ajax, XAML, Visual Basic 6.0, Visual Studio, Team Foundation Server. In addition to support the Adobe Enterprise Suite (LiveCycle) application Adobe Workbench, Java and Eclipse or similar.
APPS/R/APPDEV/002	Where Users are unable to make changes to aspects of the system then the Change Control Procedures shall be used to request such changes to be made by the Supplier. The Supplier shall assess, agree and test each request before rolling it out to Users
APPS/R/APPDEV/003	The Supplier shall implement a consistent User interface across all new systems that the Supplier provides. This shall be based around the interface provided by, where applicable, Microsoft Windows and the COTS products employed. The Supplier shall use standard features for all elements of the User interface.
APPS/R/APPDEV/004	As part of the design of systems the Supplier provides, the Supplier shall assess the suitability of COTS products for providing the required functionality. Where the product is suitable, the Supplier shall use a COTS product.
APPS/R/APPDEV/005	Where Customer requirements are such that use of COTS products are not the most cost-effective solution, the Supplier shall provide a bespoke solution, or shall tailor the COTS products to provide the required solution, or shall propose changes to business processes.

Reference ID	Requirement
	Similarly, the Supplier shall use portable and scalable technologies to allow systems to be used from different environments e.g. using desktop PCs, laptops.
APPS/R/APPDEV/006	The Supplier shall design its systems so that once data has been entered by a User, or where it has been received electronically from another source, that data shall be validated and once this has been done it will not need to be entered again. The data shall be stored in a central database and shall be accessed and shared between applications/screens.
APPS/R/APPDEV/007	NOT USED.
APPS/R/APPDEV/008	The Supplier shall ensure the distribution of data and software updates and patches will be as per vendor recommendations and implemented with 4 weeks of being made available, unless otherwise agreed with the Customer.
APPS/R/APPDEV/009	The Supplier shall maintain a change management capability to ensure that new services and associated training or other adjustments are efficiently integrated into Service Delivery when ready.

10. Testing

Reference ID	Requirement
APPS/R/TEST/001	The Supplier shall conduct testing in line with processes that adhere to Call Off Schedule 5 (Testing).
APPS/R/TEST/002	The Supplier shall observe a testing strategy that is based upon a series of testing 'phases', each linked to a particular stage in the project life-cycle. For each testing phase, the Supplier shall create various test scripts, based upon the how the system should work, including as defined in the Functional Specification.
APPS/R/TEST/003	The Supplier shall conduct, but not be limited to, the following testing life-cycle to establish the integrity of the system tested: a. Module (or Unit) testing– individual 'modules' of software are thoroughly tested for functional and technical correctness; b. Integration testing – modules which have successfully undergone module testing, are tested with each other in order to demonstrate that they integrate correctly; c. System testing – a complete system or product is fully tested for functional and technical correctness against its specifications; d. Services testing as defined in Call Off Schedule 5 (Testing). e. The Supplier shall develop test scenarios to use during the integration, system and acceptance testing phases and will seek guidance from the Customer to ensure that the scenarios are realistic.
APPS/R/TEST/004	By a combination of methodical design, and rigorous testing based upon this design, the Supplier shall validate all data entered into the

Reference ID	Requirement
	system, whether directly or as an import, before it is committed.
APPS/R/TEST/005	The Supplier shall use a combination of methodical design and rigorous testing to prove that the system acts according to how it should act including as specified in the Functional Specification. This shall include tests to show that where data transfers require authorisation, such authorisation is requested and received before transmission takes place.
APPS/R/TEST/006	NOT USED.
APPS/R/TEST/007	All testing shall be conducted using the path to Live Test Environment, and shall not be conducted within the production environment
APPS/R/TEST/008	All testing is to be signed off by the Customer via the operational change management process ahead of moving the components tested to the production environment.

11. ITA Requirements

Reference ID	Requirement
APPS/R/ITAREQ/001	The Supplier will provide consultancy to the Customer and analytical assessments themselves or shall recommend the engagement of reputable Sub-Contractors or 3rd parties The Supplier shall ensure a robust testing plan of all ITA related solutions is undertaken prior to the provision being made available to the User to reduce the likelihood of post Implementation issues.
APPS/R/ITAREQ/002	The Supplier will provide a dedicated single point of contact to work with the Customer to seek out and implement ITA solutions within agreed timescales (usually no more than 50 days from the date of the Customer raising a request or Order) and to agree an approach to undertake user testing to mitigate post Implementation issues of the provision.
APPS/R/ITAREQ/003	The Supplier will work with the Customer to agree an approach for more complex ITA requirements including continuous improvement and investigation for ITA users.
APPS/R/ITAREQ/004	When providing the Service Catalogue, the Supplier shall include ITA products and services to enable prompt delivery of recurring ITA requests.
APPS/R/ITAREQ/005	The Supplier will provide a service for new ITA requests and those inflight or previously implemented where User needs identify further requirements or fixes. This includes incident investigation and resolution relating to previously delivered ITA Software and hardware.

Reference ID	Requirement
APPS/R/ITAREQ/006	The Supplier will identify solutions to meet ITA requests, including the procurement, planning and delivery of solutions and reporting on compatibility issues of provision and Customer ITA solutions and provide options to meet the user and business needs of delivering the provision.
APPS/R/ITAREQ/007	The Supplier will build, install and test solutions to ensure compatibility where Customer hardware and software is upgraded, replaced, developed or implemented.
APPS/R/ITAREQ/008	The Supplier will provide associated training for ITA solutions to enable Users to fully utilise their solutions, at agreed times with the Users and will provide associated training materials for all provision specifically for ITA users to the Customer.
APPS/R/ITAREQ/009	The Supplier shall ensure new developments are utilised to improve the User experience, including but not limited to upgrades to Dragon and JAWS software.
APPS/R/ITAREQ/010	The Supplier will conduct quarterly end of life reviews on ITA related products supplied by the Supplier, and provide the results of such reviews including an impact assessment for the User, and where applicable, schedule User testing of any upgrades.
APPS/R/ITAREQ/011	The Supplier will build, install and test solutions to meet ITA user and business needs as part of the provision or as a separate stream only if agreed by the Customer.
APPS/R/ITAREQ/012	The Supplier will provide documentation of all ITA User needs, solutions, end of life services or support, and lessons learned.
APPS/R/ITAREQ/013	The Customer is entitled to require the Supplier to provide solutions for new or existing key ITA Users out of Working Hours.
APPS/R/ITAREQ/014	The Supplier will attend monthly reviews of the ITA service with the Customer to review the performance of the service including activity delivered or in flight; lessons learned; risks and issues outstanding; financial spend; minutes; action trackers and agree to act on any corresponding actions.

E. Security Requirements

The requirements set out under this section cover:

#	**System**
1	General Security;
2	Physical Security;
3	Architecture Security;
4	Encryption
5	Environment Protective Monitoring;
6	Environment Identity and Access Management
7	Anti Virus and Malware
8	Vulnerability Management
9	Remote Access Security; and
10	Security Architecture and Design

In the event that there is a conflict between this section and the information contained within Call Off Schedule 8 (Security), this section shall take precedence.

1. General Security

Reference ID	**Requirement**
APPS/R/GENSEC/001	The Supplier shall provide the Customer access to Supplier Personnel and Supplier premises as required for the purposes of improving and auditing security.
APPS/R/GENSEC/002	The Supplier shall provide that its firewalls provide the ability to undertake security event audit logging.
APPS/R/GENSEC/003	The Supplier shall ensure that named User accounts used by the Supplier's support personnel for server support shall have specific roles/privileges. Generic unnamed administrative accounts will not be allowed unless explicitly authorised by the Customer's Accreditor.
APPS/R/GENSEC/004	The Supplier shall ensure that the equipment used to provide the Supplier's inter-site links shall be sufficiently secure from tampering and shall alert the operations bridge to a sufficient degree of attempted tampering on the basis that the information carried is protectively marked no higher than OFFICIAL-SENSITIVE.
APPS/R/GENSEC/005	The Supplier Solution shall be designed so that it conforms to the security and audit requirements defined in Call Off Schedule 8 (Security).
APPS/R/GENSEC/006	Physical measures shall be taken by introducing additional firewalls onto the Customer WAN to prevent unauthorised access to the Customer network from external threat;

Reference ID	Requirement
APPS/R/GENSEC/007	ATI (advanced threat investigation) The Customer requires a specialist threat based analytics service to augment the Customer's protective monitoring capability. This needs to draw information from the Customer security systems and provide a combination of expert oversight and automated analytics, to detect and respond to advanced network threats and provide malware analysis capabilities
APPS/R/GENSEC/008	The Supplier shall carry out regular IT Health Checks (at a frequency to be agreed during Implementation) and present the outcome of such health checks to the Customer
APPS/R/GENSEC/009	The Supplier shall make available their Security Management Plan as and when required by the Customer and keep it up to date
APPS/R/GENSEC/010	The Supplier shall demonstrate evidence of Protective Monitoring
APPS/R/GENSEC/011	The Supplier will demonstrate, through a Customer authorised third party, that the infrastructure has been penetration tested, ensuring security and reliability.

2. Physical Security

Reference ID	Requirement
APPS/R/PHYSSEC/001	The Supplier shall operate policies and procedures for the hosting environment that support the operation of a safe and secure working environment in offices, rooms, facilities, and secure areas storing / processing Customer Data.
APPS/R/PHYSSEC/002	The Supplier shall ensure that all Assets identified in Call Off Schedule 9 (Software and Assets) operated by the Supplier to support the hosting of Customer Data and systems must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of all assets utilized to facilitate the hosting of Customer operations shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.
APPS/R/PHYSSEC/003	The Supplier shall deploy a combination of physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance (including CCTV), physical authentication mechanisms, reception desks, and security patrols) to safeguard Customer Data and systems.
APPS/R/PHYSSEC/004	Access to areas containing Customer Data, systems and

Reference ID	Requirement
	services shall be controlled and monitored by physical access control mechanisms to ensure that only authorized Supplier Personnel are allowed access.
APPS/R/PHYSSEC/005	The Supplier shall manage access to its wider hosting site, such as service areas and other points where unauthorized personnel may enter the premises. These shall be monitored, controlled and isolated from systems hosting Customer Data and services to prevent unauthorized data corruption, compromise, and loss. Authorisation shall be obtained from the Customer prior to relocation or transfer of any element of the hosted solution to offsite / alternative premises.
APPS/R/PHYSSEC/006	The Supplier shall provide assurance on the effectiveness of the physical security of its hosting arrangements through external validation against a recognized and relevant security standard. The Supplier shall provide evidence of the successful external validation to the Customer prior to seeking the first Milestone Payment on the Implementation Plan, and at the Customer's reasonable request.
APPS/R/PHYSSEC/007	The Supplier shall deliver a range of environmental controls aligned to recognized best practice which as a minimum shall include temperature and humidity management, fire identification and suppression, static electricity monitoring and power management and resilience.

3. Architecture Security

Reference ID	Requirement
APPS/R/ARCSEC/001	The Supplier shall ensure that all hosting infrastructure handling, storing and processing the Customer's information undergoes an accreditation / assurance process in accordance with the Customer's Accreditation / Assurance Strategy.
APPS/R/ARCSEC/002	The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and User access to the minimum possible level) to the design and configuration of the hosting infrastructure that will process or store Customer Data.
APPS/R/ARCSEC/003	The Supplier shall develop, implement and maintain a security governance framework that coordinates and directs its overall approach to the management of the hosting environment and the information processed (e.g. ISO27001 registration / certification).
APPS/R/ARCSEC/004	The Supplier shall develop, implement and maintain 'Processes and Procedures' to ensure the operational security of the hosting environment. Such Processes and Procedures shall be formally documented and reflected in ISMS procedures that would

Reference ID	Requirement
	support ISO27001 registration / certification.
APPS/R/ARCSEC/005	The Supplier shall ensure that its Supplier Personnel are subject to: (i) adequate personnel security screening; and (ii) adequate security education to ensure that they are able to perform their role.
APPS/R/ARCSEC/006	The Supplier shall design and develop services to identify and mitigate threats to security and any risks that such threats may present to Customer Data.
APPS/R/ARCSEC/007	The Supplier shall ensure that its supply chain supports (to the satisfaction of the Customer) all of the security principles that the hosting solution claims to implement.
APPS/R/ARCSEC/008	The Supplier shall ensure that, where applicable, the Customer and/or its Agency Manager is provided with the tools required to take appropriate action on any issues or risks that may arise (such as, access to audit and log information to support incident investigation). The Supplier shall ensure that a forensic readiness capability is consistently provisioned in accordance with the requirements of CESG Good Practice Guide No.18 – Forensic Readiness and that it reflects the sensitivity of Customer Data.
APPS/R/ARCSEC/009	The Supplier shall be responsible for security hardening of the hosting infrastructure. Operating systems shall be hardened to provide only necessary ports, protocols, and services to meet Customer business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard.
APPS/R/ARCSEC/010	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is embedded within the hosting environment and at its perimeter and interfaces with any other network, service, applications or devices.
APPS/R/ARCSEC/011	The Supplier shall provide boundary controls within the hosting infrastructure and identify and confirm the security of all connectivity aspects associated with the Customer hosting environment. Separation and segregation shall be achieved by a combination of physical and technical arrangements that have been Approved by the Customer.
APPS/R/ARCSEC/012	Access to all management functions or administrative consoles for systems hosting Customer Data shall be restricted to authorized personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS

Reference ID	Requirement
	encapsulated communications to the administrative consoles).
APPS/R/ARCSEC/013	The Supplier shall establish a change and configuration control process for the hosting environment to: a. Prevent installation of unauthorised software; b. Update & patch known security vulnerabilities in a timely manner; c. Test all patches and updates prior to deployment; d. Implement work-rounds / other controls where delays in fixing vulnerabilities occur.
APPS/R/ARCSEC/014	The Supplier shall: a. Provide the Customer with all Customer Data on demand in an agreed open format; b. Have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade; c. Securely destroy all media that has held Customer Data at the end of life of that media in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor); and d. Securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor).
APPS/R/ARCSEC/015	The Supplier shall make available to the Customer and its designated agents any reasonably requested resources including physical access to Sites, facilities and Key Personnel that support the delivery of the services provided.
APPS/R/ARCSEC/016	The Supplier shall adhere to and directly support compliance with, all relevant 'Codes of Connection' for services accessed by the Customer from the hosting environment.
APPS/R/ARCSEC/017	The Customer and Supplier shall recognise the need for information to be safeguarded under the UK and EU Data Protection regime (including all relevant aspects of GDPR). To that end, the Supplier shall be able to state to the Customer the physical locations in which data may be hosted from, and to confirm that all relevant legal and regulatory frameworks are complied with.
APPS/R/ARCSEC/018	The Supplier shall be responsible for the scope and delivery of IT Healthchecks / Penetration Testing to the satisfaction of the Customer. The Supplier shall offer necessary assistance should the Customer determine that they require additional / independent IT Healthchecks as frequently as reasonably

Reference ID	Requirement
	required by the Customer. All IT Healthchecks / Penetration Testing shall be delivered by a CHECK 'Green' penetration testing service provider.
APPS/R/ARCSEC/019	The Supplier shall develop a Business Continuity Plan (BCP) and Disaster Recovery arrangements incorporating risks identified in a risk assessment, including malicious, accidental, technical failure and natural events that could disrupt the Customer's business that is reliant upon the services provided by the hosting environment. The plans shall reflect Customer Recovery Time Objectives (RTOs).

4. Encryption

Reference ID	Requirement
APPS/R/ENCRYP/001	The Supplier shall provide encryption of data at rest that resides within the hosting environment and that which is stored as 'back up' using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (NCSC and formerly CESG) to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA"). Should the Supplier elect to deploy a 'non assured' product, then this shall be Approved by the Customer.
APPS/R/ENCRYP/002	The Supplier shall ensure that data passed between the hosting environment and any other location of access should be similarly encrypted whilst in transit. In the event that the Supplier determines that the risk which encryption mitigates against is managed by some other means, then this shall be formally recorded. In such circumstances, the Customer will, taking full account of 'residual risk,' determine whether the alternative means of data protection are acceptable. The Supplier solution shall comply with relevant CESG (now NCSC) cryptographic policy, specifically Cryptographic Mechanisms, Algorithms and Protocols, and apply relevant cryptographic assurance requirements (including operational and physical requirements) for the implementation of cryptographic mechanisms (signing certificates and CRLs), the protection of signing keys, the protection of interactions between service elements and the protection of interactions between Case Allocation services and external elements.

5. Environment Protective Monitoring

Reference ID	Requirement
APPS/R/ENVIRO/001	The Supplier shall deliver a Protective Monitoring regime that is compliant with the requirements of CESG Good Practice Guide No13 – Protective Monitoring for HMG ICT Systems. The solution shall ensure that threats associated with DDOS, MITM, IP Spoofing, Port Scanning, packet sniffing are covered, along with threats that may be 'internal' such as from any party that may have access to hosting arrangements.
APPS/R/ENVIRO/002	The Supplier's Protective Monitoring regime shall provide centralized collection, analysis and correlation of information that is generated by security enforcing technologies such as firewalls, IDS/IPS, AV logs etc that relate to the hosting arrangements provided for the Customer.
APPS/R/ENVIRO/003	The Supplier shall ensure the existence of 'accurate time logs' through as a minimum, the provision of a master time source and synchronisation of all device clocks, time stamping of event records and time stamping of alert messages.
APPS/R/ENVIRO/004	The Supplier shall monitor, record, analyse and report upon business traffic crossing the boundaries of the hosting environment, to ensure that such traffic is authorised and in accordance with security policy. Minimum requirements include: a. Malware detection at the perimeter firewall and internal firewall arrangements; b. Reporting of blocked file import attempts at the firewall; c. Reporting of blocked file export attempts at the firewall; d. Reporting of allowed file import at the firewall; e. Reporting of allowed file export at the firewall.
APPS/R/ENVIRO/005	The Supplier shall monitor, record, analyse and report upon activity at the boundary of the hosting environment with a view to detecting suspicious activity. Minimum requirements include: a. Recording packets dropped by boundary firewalls; b. Deployment of IDS along with an appropriate alerting system; c. Recording of suspected attacks and centralized reporting; d. Recording of changes to firewall (and similar) rule sets with activities of Users involved in making changes logged.
APPS/R/ENVIRO/006	The Supplier shall detect changes to all device status and configurations that form part of the hosting service provided. Minimum requirements include: a. Reporting of Critical host messages; b. Host malware detection records; c. Recording of changes to anti malware signature base; d. Logging and reporting of failed file system access

Reference ID	Requirement
	attempts; e. Recording of changes to access rights on system folders/directories; f. Recording of change of status in hosts, attached devices and storage volumes; g. Recording of changes to system (registry) or software configuration; h. Recording of changes to files within system folders.
APPS/R/ENVIRO/007	The Supplier shall monitor internal boundaries and segregations within the hosting environment to detect suspicious activities. Minimum requirements include: a. Reporting of dropped packets at internal firewalls; b. Deployment of IDS within the hosting environment incorporating virtualized aspects; c. Recording of packets passed by internal firewalls; d. Internal system monitoring events at 'critical' or above; e. Authentication failures; f. System console messages at 'error' status; g. Changes to firewall rule sets; h. User sessions on devices.
APPS/R/ENVIRO/008	The Supplier shall monitor any temporary connections to the hosting environment made by remote access, VPN or other transient means of connection. Minimum requirements include the recording of: a. Successful sessions; b. All unsuccessful VPN connections; c. Authentication failures; d. Wireless connections (attempted and successful); e. Changes in VPN configuration; f. Authentication failures; g. Change in status of IDS.
APPS/R/ENVIRO/009	The Supplier shall monitor User/administrator activity and access to ensure accountability and detect unauthorised activity. Minimum requirements include the recording of: a. User sessions; b. User account status changes; c. Changes to privileges; d. Use of database or application administration facilities; e. Running of commands and executables.
APPS/R/ENVIRO/010	The Supplier shall ensure that Critical classes of events are notified in as close to 'real time' as possible. Minimum requirements include the recording of: a. Alert messages routed to Supplier security console; b. Secondary channel alerting, e.g. SMS messaging. c. The solution shall also allow for the provision of

Reference ID	Requirement
	customized performance metrics to be reported to the Customer.

6. Environment Identity and Access Management

Reference ID	Requirement
APPS/R/ENVID/001	The Supplier shall operate access control policies and procedures and supporting business processes and technical measures, for ensuring appropriate identification and authentication of personnel involved in the administration of the hosting environment.
APPS/R/ENVID/002	The Supplier shall deliver solution that reduces the number of different access arrangements that Users have in support of the corporate objective of 'Single Sign On' (SSO).
APPS/R/ENVID/003	The Supplier shall define procedures and confirm roles and responsibilities for provisioning and de-provisioning of administrative User accounts following the rule of least privilege, based on defined job function.
APPS/R/ENVID/004	The Supplier shall provide User account management, delivering the following: a. A centralised process to authorise the creation and deletion of a User account; b. Full visibility (to authorised personnel) in a single place, on who has access to which resource; c. Ability to ensure that proposed new Users do not already have accounts elsewhere; d. Facilitate changes on a 'group' basis rather than at the individual User level.
APPS/R/ENVID/005	The Supplier shall provide all Users with visibility of the resources they have been granted access to and to those that they may be able to request access to in order to work more effectively.
APPS/R/ENVID/006	The Supplier shall support simple 'job movement' by allowing Users who change their jobs / roles to be able to retain the same access credentials with updates taking place in the background.
APPS/R/ENVID/007	The Supplier shall ensure that 'authentication' is risk based and supported by a centralised policy framework. The policy framework shall allow for the deployment of multifactors for authentication, which can be augmented as a result of the sensitivity and/or risk to the hosting environment at any given time. Any authentication system / product used shall allow for the deployment of 3rd party factors.
APPS/R/ENVID/008	The Supplier shall identify, assess, and prioritize risks associated with any third-party access to the hosting environment by

Reference ID	Requirement
	coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Risk management controls shall be implemented prior to providing access to any third party.
APPS/R/ENVID/009	The Supplier shall ensure timely de-provisioning of administrator access to the hosting environment in accordance with established policies in the event of change to a User's status (e.g., termination of employment or other business relationship, job change, or transfer).
APPS/R/ENVID/010	The Supplier shall provide centralized administration of the ID&AM regime for the hosting environment. Centralized administration shall deploy management tools in order to have complete visibility of the ID&AM regime.
APPS/R/ENVID/011	The Contactor shall ensure that administrative Users are managed through a centralised policy driven approach. Privileges shall be allocated and managed using a centralised management facility, which provides visibility and control of systems and services that Users have access to.
APPS/R/ENVID/012	The Contactor shall ensure that 'privileged Users' are managed in the same way as any User, through a centralised policy driven approach. Privileges shall be allocated and managed using a centralised management facility, which provides visibility and control of systems and services that privileged Users have access to.
APPS/R/ENVID/013	The Supplier shall implement an ID&AM regime that deploys a centralised function to monitor and report activity including: a. Suspicious login attempts / failed logins; b. Monitor access patterns; c. Allowing for tailored and scalable monitoring of User / activities when required; d. Identify unknown / unrecognised access devices and locations; e. Centralised logging and analysis of 'security events'.
APPS/R/ENVID/014	The Supplier shall ensure that access to, and use of, audit tools that support the operation of the hosting environment's identity and access management regime shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.
APPS/R/ENVID/015	The Supplier shall implement an ID&AM regime that maintains security and event related information in a manner that ensures forensic integrity is retained. Arrangements shall support swift intervention following the identification of an incident, which allows for example, immediate suspension of an account across all instance of its use. The Supplier shall be responsible for integration into wider Customer incident response procedures, in order to ensure a consistent response irrespective of incident type.
APPS/R/ENVID/016	The Supplier shall provide a service for Directory Services centralised access requests. Whilst 'automation' is an accepted

Reference ID	Requirement
	enabling objective, the Supplier shall ensure that this process does not undermine the requirement for appropriate business authorisation of access requests.
APPS/R/ENVID/017	The Supplier shall deliver centralisation of Directory Services providing a single interface to manage all Users, groups and devices that are within the scope of the services provided. This single interface shall deliver integration, deal with requests from applications and directories and support effective password management through application of policy requirements.

7. Anti Virus and Malware

Reference ID	Requirement
APPS/R/ANTVIR/001	The Supplier shall ensure that applications are protected through an holistic anti-virus and malware prevention and detection regime that delivers layered security against this threat. Additionally, the Supplier shall provide controls for protecting applications against Advanced Persistent Threats (APTs).
APPS/R/ANTVIR/002	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is applied both within the application environment and at its perimeter and interfaces with any other network, service, application or device.
APPS/R/ANTVIR/003	The Supplier shall employ automated tools to continuously monitor all services that are provisioned within the application environment for virus and all forms of malware. All malware detection events shall be centrally collated, managed and logged.
APPS/R/ANTVIR/004	The anti-virus and malware prevention and detection regime shall deploy modern AV/Malware protection that provides assurance on its capability to detect, remove and protect against all 'known' types of Malicious Software.
APPS/R/ANTVIR/005	The Supplier shall maintain the anti-virus and malware prevention and detection regime so that it is updated in accordance with extant threat levels. Updates to software supporting the regime shall take place on both a scheduled and threat informed basis.
APPS/R/ANTVIR/006	The Supplier shall ensure that updates to the malware prevention and detection regime are pushed out to all services that are provisioned within the scope of this Call Off Contract in a consistent and timely manner.
APPS/R/ANTVIR/007	The Supplier shall ensure that its process to download and distribute updates to the anti-virus malware prevention and detection regime does not introduce threats to the application environment. The Supplier shall ensure that all updates are verified and are free from malicious content prior to introduction to the application environment.

Reference ID	Requirement
APPS/R/ANTVIR/008	The Supplier's malware prevention and detection regime shall be integrated with the Customer's wider incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.

8. Vulnerability Management

Reference ID	Requirement
APPS/R/VUNMAN/001	The Supplier shall deliver a Vulnerability Management regime that provides assurance to the Customer that all potential new threats, vulnerabilities or exploitation techniques, which could affect the hosting environment are assessed and corrective action is taken.
APPS/R/VUNMAN/002	The Supplier shall monitor relevant sources of information relating to threat, vulnerability and exploitation techniques, in order to support the provision of an appropriately informed Vulnerability Management regime.
APPS/R/VUNMAN/003	The Supplier shall consider the severity of threats taking full account of the criticality of Customer Data and services that are hosted in the prioritization of mitigation implementation.
APPS/R/VUNMAN/004	The Supplier shall track all identified vulnerabilities and monitor them until required mitigations have been deployed. Timescales for implementing mitigations to vulnerabilities found within the hosting environment shall be communicated to the Customer.
APPS/R/VUNMAN/005	The Supplier shall act immediately to put mitigations in place for any vulnerability where evidence suggests that it is being exploited 'in the wild'. If there is no evidence that the vulnerability is being actively exploited, and where there is no vendor recommendation then the following timescales shall be considered minimum good practice: *'Critical' patches deployed within 14 calendar days of a patch becoming available*
APPS/R/VUNMAN/006	The Supplier shall provide 'real time' vulnerability scanning and remediation deploying best-in-class Vulnerability Management solutions that deliver comprehensive discovery, tailored to the modern, constantly evolving threat environment.
APPS/R/VUNMAN/007	The Supplier shall provide a Vulnerability Management regime that includes within its scope all assets that fall within the scope of the hosting service being provisioned.

Reference ID	Requirement
APPS/R/VUNMAN/008	The Supplier shall deliver a Vulnerability Management regime that supports automatic and tailored adjustment of the analysis process, which takes account of changes to the Customer's risk, threat and vulnerability profile.
APPS/R/VUNMAN/009	The Supplier shall undertake appropriate Root Cause analysis of identified vulnerabilities, in order to learn from the mitigation process, to limit the possibility of recurrence. This shall contribute to a pro-active approach to Vulnerability Management that is not limited to simply responding to events.
APPS/R/VUNMAN/010	The Supplier shall provide a Vulnerability Management regime in accordance with these requirements that is consistent for all elements of the hosting service provided
APPS/R/VUNMAN/011	The Supplier shall provide the Customer with a monthly summary report on the 'threat landscape'. This report shall include an analysis of metrics that provides the Customer with an understanding of the threats the Supplier has managed and is facing and should not simply be a summary of statistical information. The Supplier shall undertake intelligent analysis in order to provide the Customer with meaningful information to help determine the assurance profile.
APPS/R/VUNMAN/012	The Supplier's Vulnerability Management regime shall be integrated with the Customer's wider incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.
APPS/R/VUNMAN/013	The Supplier shall be responsible for the arrangement, delivery and associated costs of all external vulnerability testing (penetration testing / IT Healthchecks) that are required to support the accreditation/assurance requirements of the hosting environment, as determined by the Customer. All independent testing undertaken shall be delivered by an approved organization, normally CHECK. Any independent testing that is not carried out by a CHECK approved company, shall be explicitly authorized by the Customer.

9. Remote Access Security

Note: The words in inverted commas in this section 9 and section 10 below are standard security phraseology.

Reference ID	Requirement

Reference ID	Requirement
APPS/R/RAS/001	The Supplier shall provide remote access services that are consistent with guidance provided in the document, CESG Architectural Patterns – Walled Gardens for Remote Access.
APPS/R/RAS/002	The Supplier shall provide assured data-in-transit protection. This shall include the deployment of an IPsec client that is assured to 'Foundation Grade' under CESG's Commercial Product Assurance (CPA) scheme. This assurance shall be against the CESG's IPsec VPN for Remote Working – Software Client (SC) Security Characteristic, configured in accordance with PSN end-state IPsec profile or PSN interim IPsec profile.
APPS/R/RAS/003	The Supplier shall define an 'Access Layer' within a DMZ arrangement, where clients are authenticated and termination of the cryptographic link takes place. A firewall shall be deployed to ensure that only approved VPN traffic can reach the 'gateway'. The 'Access Layer' shall provide protection against network bound attacks such as DDoS.
APPS/R/RAS/004	If required, the Supplier shall define a 'Presentation Layer' for an agreed subset of web-based application services to the remote access device. The 'Presentation Layer' shall reside within a DMZ. For such agreed subset, remote access devices shall connect to proxying arrangements and not directly to core application services. .
APPS/R/RAS/005	The Supplier shall provide assured data-at-rest protection. Any data stored on remote access devices shall be encrypted with an encryption product that is assured to 'Foundation Grade' under CESG's Commercial Product Assurance (CPA) scheme. This shall be deployed when the device is in its 'rest' state. For 'always on' devices, this encryption shall be deployed when the device is locked.
APPS/R/RAS/006	The Supplier shall deploy an effective authentication process for all devices and the services they access which should include the following aspects: • User to device, whereby the User shall only be granted access to the device following successful authentication to the device; • User to service, whereby the User shall only be able to access services after successful authentication to the service via their device; • Device to service, whereby devices are only granted access following successful authentication to the application environment.
APPS/R/RAS/007	The Supplier shall deploy 'platform integrity and application sandboxing'. Arrangements shall ensure that the remote access

Reference ID	Requirement
	device can continue to operate securely in the event of a compromise of an application or component within the platform. Functionality shall support the requirement to restrict the capabilities of applications on the device.
APPS/R/RAS/008	The Supplier shall deploy 'malicious code detection and prevention' controls for the remote access service. Arrangements shall detect, isolate and defeat malicious code, which may have achieved ingress to the remote access architecture.
APPS/R/RAS/009	The Supplier shall ensure effective 'security policy enforcement' to ensure that policies set by the enterprise are implemented in remote access devices. It shall be possible to centrally enforce a set of security policies on devices and ensure that these policies cannot be circumvented by the device User or unauthorised entity.
APPS/R/RAS/010	The Supplier shall deploy 'external interface protection' ensuring that remote access devices are limited to an agreed profile, the number of ports (physical and logical) and services exposed to untrusted networks and devices.
APPS/R/RAS/011	The Supplier shall deploy 'event collection' for all elements of the remote access service, to report security events to a centrally provisioned audit and monitoring arrangement. This facility shall be restricted from the User and mitigate against unauthorised access attempts.
APPS/R/RAS/012	The Supplier shall deploy an 'incident response' arrangement that integrates with wider response procedures in place across the Customer ICT Environment.

10. Security Architecture and Design

Reference ID	Requirement
APPS/R/SECARC/001	The Supplier shall ensure that all systems / applications handling, storing and processing the Customer's information undergo an accreditation / assurance process in accordance with the Customer's Accreditation / Assurance Strategy.
APPS/R/SECARC/002	The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and User access to the minimum possible level) to the design and configuration of systems / applications / services which will process or store Customer Data (aka Designated Access Rights).

Reference ID	Requirement
APPS/R/SECARC/003	The Supplier shall ensure that any transmission of Customer Data is adequately protected against tampering, denial of service, eavesdropping and virus ingress.
APPS/R/SECARC/004	The Supplier shall ensure that Customer Data (and the assets storing or processing such Customer Data), shall be adequately protected against physical tampering, loss, theft, damage or seizure.
APPS/R/SECARC/005	The Supplier shall ensure that an adequate degree of separation exists between different Users of the services provided by the systems / applications. This should prevent anyone malicious or compromised from affecting the provision of the services or the security of Customer Data.
APPS/R/SECARC/006	The Supplier shall develop, implement and maintain a security governance framework that coordinates and directs its overall approach to the management of the systems / applications / services and the information processed (e.g. ISO27001 registration / certification).
APPS/R/SECARC/007	The Supplier shall develop, implement and maintain 'Processes and Procedures' to ensure the operational security of the services provided. Such Processes and Procedures shall be formally documented and reflected in ISMS procedures that would support ISO27001 registration / certification.
APPS/R/SECARC/008	The Supplier shall ensure that Supplier Personnel are subject to: (i) adequate personnel security screening; and (ii) adequate security education to ensure that they are able to perform their role.
APPS/R/SECARC/009	The Supplier shall design and develop services to identify and mitigate threats to security and any risks that such threats may present to Customer Data.
APPS/R/SECARC/010	The Supplier shall ensure that its supply chain supports (to the satisfaction of the Customer) all of the security principles that the Supplier Solution claims to implement.
APPS/R/SECARC/011	The Supplier shall ensure that, where applicable, the Customer and/or its Agency Manager is provided with the tools required to help the Customer securely manage the services and to take appropriate action on any issues or risks that may arise (such as, access to audit and log information to support incident investigation). The Supplier shall ensure that a forensic readiness capability is consistently provisioned in accordance with the requirements of CESG Good Practice Guide No.18 – Forensic

Reference ID	Requirement
	Readiness and that it reflects the sensitivity of Customer Data.
APPS/R/SECARC/012	The Supplier shall ensure that access to all Service interfaces is limited to authenticated and authorised Users only.
APPS/R/SECARC/013	The Supplier shall ensure that all external or less trusted interfaces of the system / application / service are identified and have appropriate protections to defend against attacks through such interfaces. These protections shall be configured in accordance with architectural arrangements outlined in CESG Good Practice Guide No.8 – Protecting External Connections to the Internet.
APPS/R/SECARC/014	The Supplier shall ensure that the methods used by Supplier Personnel to manage the services provided, mitigates any risk of exploitation that could undermine the security of the services and provides full accountability for their activities.
APPS/R/SECARC/015	The Supplier shall be responsible for the scope and delivery of IT Healthchecks / Penetration Testing to the satisfaction of the Customer. The Supplier shall offer necessary assistance should the Customer determine that they require additional / independent IT Healthchecks as frequently as reasonably required by the Customer. All IT Healthchecks / Penetration Testing shall be delivered by a CHECK 'Green' penetration testing service provider.
APPS/R/SECARC/016	The Supplier shall put in place technical policies and controls which include patching (within vendor-recommended timeframes) against known vulnerabilities. The Supplier shall ensure that security vulnerabilities and weaknesses are reported to the Customer.
APPS/R/SECARC/017	The Supplier shall make available to the Customer and its designated agents any reasonably requested resources including reasonable physical access to Sites, facilities and Key Personnel that support the delivery of the services provided.
APPS/R/SECARC/018	The Supplier shall adhere to and directly support compliance with, all relevant 'Codes of Connection' for services accessed by the Customer.
APPS/R/SECARC/019	The Customer and Supplier shall recognise the need for information to be safeguarded under the UK and EU Data Protection regime (including all relevant aspects of GDPR). To that end, the Supplier shall be able to state to the Customer the physical locations in which data may be stored, processed and managed from, and to confirm that all relevant legal and

Reference ID	Requirement
	regulatory frameworks are complied with.
APPS/R/SECARC/020	The Supplier shall agree any change in location of data storage, processing and administration with the Customer in advance where the proposed location is outside the UK. The Supplier shall be aware of legal requirements regarding the location of data outside of the UK.
APPS/R/SECARC/021	The Supplier shall: a. Provide the Customer with all Customer Data on demand in an agreed open format; b. Have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade; c. Securely destroy all media that has held Customer Data at the end of life of that media in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor); and d. Securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor). The Supplier shall establish a configuration control process to: a. Prevent installation of unauthorised software; b. Update & patch known security vulnerabilities in a timely manner; c. Test all patches and updates prior to deployment; d. Implement work-rounds / other controls where delay in fixing vulnerabilities. The Supplier shall develop a Business Continuity Plan (BCP) incorporating risks identified in a risk assessment, including malicious, accidental and natural events that could disrupt the Customer's business. The BCP shall reflect Customer Recovery Time Objectives (RTOs).

CATEGORY 3: AGENCY MANAGEMENT REQUIREMENTS

Background / Scope

The Agency Manager is responsible for managing the delivery and performance of the Services under this Call Off Contract in accordance with the terms and conditions of this Call Off Contract, including managing the Customer's governance function in relation to such delivery and performance.

The Agency Manager assists the Customer in relation to contract administration (including change management, verification of invoices and payment, etc.,) and supplier relationship management in connection with this Call Off Contract. The Supplier shall work with, respond to, cooperate with and assist the Agency Manager in relation to such contract administration and supplier relationship management.

The Agency Manager Service Requirements set out in this Category 3 of Part A of this Call Off Schedule allow the Supplier to fulfil the Supplier's obligations relating to interfacing, working with and complying with the instructions and requirements of the Agency Manager, including utilising and aligning the Services and the delivery and performance of the same with the Polices, Processes, Procedures (PPP) of the Agency Manager. The Supplier shall ensure that the Supplier PPP and the SOM align with the provisions of the Agency Manager's PPP.

In the event of a conflict, the Agency Manager's PPPs shall take precedence over the Supplier PPPs and the SOM. Therefore, the Customer is entitled to require the Supplier to cooperate with or modify the Supplier PPPs to ensure continual alignment with the Agency Manager's PPPs.

Category 3 of Part A of this Call Off Schedule contains the following Service Requirements:

1. Service Operations
    - 1.1 Service Desk
    - 1.2 Incident Management
    - 1.3 Request Management
    - 1.4 Problem Management
    - 1.5 Access Management

2. Service Design
    - 2.1 Availability Management
    - 2.2 Capacity Management

3. Service Implementation
    - 1.1 Change Management
    - 1.2 Software Asset and Configuration Management (SACM)
    - 1.3 Knowledge Management
    - 1.4 Service Transition

4. I.T. Services Continuity Management (ITSCM)

5. Service Design
    - 5.1 Service Catalogue Management
    - 5.2 Service Level management

6. Continual Service Improvement

1 SERVICE OPERATIONS

1.1 Service Desk

Reference ID	Requirement
APPS/R/SDESK/001	The Supplier shall adhere to: (i) the Service Desk Policies, Processes and Procedures; and (ii) guidance on interfacing with the Service Desk as provided to the Supplier by the Agency Manager which may be amended via Call Off Schedule 14 (Change Control Procedure).
APPS/R/SDESK/002	The Supplier shall interface with the Service Desk such that the Supplier is able to access the Service Desk tool, receive incident records logged by the Service Desk, update, amend and pass back incident records to the Service Desk as necessary.
APPS/R/SDESK/003	The Supplier shall interface with the Service Desk such that the Supplier is able to access the Service Desk tool, receive Service Catalogue requests logged by the Service Desk, update, amend and pass back request related records to the Service Desk as necessary**.**
APPS/R/SDESK/004	The Supplier shall ensure that, where necessary, the interfaces between the Supplier Systems and the Service Desk shall be automated to allow tickets to be raised automatically between the Supplier Systems and the Service Desk tool
APPS/R/SDESK/005	The Supplier shall provide advice and support to the Customer's staff and Users on the operation of the Supplier Solution.
APPS/R/SDESK/006	The Supplier shall provide feedback to Users and /or the Agency Manager on progress made with resolving an Incident. Such feedback shall include: (i) advice on any remedial action being taken; (ii) the estimated date and time when the Incident may be Resolved; (iii) and advice allowing the User to continue to use the Services until such time as the Incident is Resolved.
APPS/R/SDESK/007	NOT USED.
APPS/R/SDESK/008	The Supplier shall develop Application Support and data hosting PPPs for the delivery of the Services.
APPS/R/SDESK/009	The Supplier shall interface with the Service Desk provided by the Agency Manager such that the Supplier is able to receive Incident and requests records logged by the Service Desk, update, amend and pass back incident records to the Service Desk as necessary.

Reference ID	Requirement
APPS/R/SDESK/010	The Supplier shall contribute to the Knowledge Management System and the Known Error Log provided by the Agency Manager to support improved Incident analysis.
APPS/R/SDESK/011	NOT USED
APPS/R/SDESK/012	The Supplier shall ensure that Root Causes to Incidents and problems are addressed, and that Workarounds that continue to exist while the Root Cause is addressed are reported each Service Reporting Period.

1.2 Incident Management

Reference ID	Requirement
APPS/R/INCMAN/001	The Supplier shall investigate and resolve all Incidents in accordance with the Service Levels, including: a. assessing the probable cause of each Incident; b. testing and replacing or repairing faulty hardware/software as required; and c. carrying out any other procedures as required to facilitate the resolution of the Incident.
APPS/R/INCMAN/002	Where an Incident relates to security, the Supplier shall maintain the forensic integrity of systems following an incident in accordance with good practice defined within 'CESG Good Practice Guide No 18 – Forensic Readiness'.
APPS/R/INCMAN/003	The Supplier shall promptly complete agreed corrective actions as agreed with the Agency Manager.
APPS/R/INCMAN/004	The Supplier shall promptly notify the Agency Manager of any Incident that is known to have breached or is likely to breach the Service Levels or that has, in the opinion of the Supplier, been incorrectly allocated.
APPS/R/INCMAN/005	The Supplier shall; (i) update the Incident record with all relevant information to ensure that Root Cause analysis can be carried out by the Agency Manager; and (ii) co-operate with the Agency Manager as required for the Agency Manager to carry out Root Cause analysis.
APPS/R/INCMAN/006	Where the Agency Manager has altered the assigned Incident Severity Level of an Incident in accordance with Customer instructions and agreed this with the Supplier, the Supplier shall resolve such Incident in accordance with the new Incident Severity Level.

Reference ID	Requirement
APPS/R/INCMAN/007	The Supplier shall ensure that, in the event that the investigation of an Incident reveals non-compliance of the Supplier Solution with any Requirement set out in this Call Off Contract, then the Supplier shall rectify such non-compliance at no cost to the Customer. Such rectification shall be Approved by the Customer and the Agency Manager, in advance and, where necessary, implemented via the Change Control Procedure.

1.3 Request Management

Reference ID	Requirement
APPS/R/REQMAN/001	The Supplier shall contribute to and use the Business Service Catalogue including in accordance with the relevant PPP.
APPS/R/REQMAN/002	The Supplier shall review Management Information on a monthly basis to identify trends or significant changes or increases in service request volumes, for discussion with the Agency Manager and, where necessary, Related Suppliers, as applicable.
APPS/R/REQMAN/003	The Supplier shall identify possible Process improvements and promptly make appropriate recommendations to the Agency Manager in writing.
APPS/R/REQMAN/004	The Supplier shall immediately bring to the attention of the Agency Manager any issues that prevent the Supplier from processing Service Requests.
APPS/R/REQMAN/005	The Supplier shall ensure that Service Requests received from the Agency Manager are expedited within agreed Service Levels when assigned by the Service Desk
APPS/R/REQMAN/006	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Agency Manager in response to Service Requests.
APPS/R/REQMAN/007	The Supplier shall: (i) co-operate with the Agency Manager to proactively manage and monitor the status and progress of all Service Requests for the Services ordered via the Business Service Catalogue; and (ii) adhere to the PPP relevant to Service Requests as provided by the Agency Manager.
APPS/R/REQMAN/008	The Supplier shall respond to the Agency Manager or the

Reference ID	Requirement
	Customer's enquiries regarding Service Requests with accurate and up-to date information.
APPS/R/REQMAN/009	NOT USED.

1.4 Problem Management

Reference ID	Requirement
APPS/R/PROBMAN/001	The Supplier shall adhere to the problem management policies, processes and procedures as set out in the Agency Manager's Problem Management Procedure
APPS/R/PROBMAN/002	The Supplier shall participate with the Agency Manager in Incident Reviews and Major Incident Reviews, as necessary
APPS/R/PROBMAN/003	The Supplier shall (i) contribute to Major Incident Reports; and (ii) ensuring that Major Incident Reports provide clear details to the Agency Manager as set out in the Problem Management Procedure.

1.5 Access Management

Reference ID	Requirement
APPS/R/ACCMAN/001	The Supplier shall provide access to systems as requested by the Users in accordance with: (i) the Policies of the Customer and/or Agency Manager relating to Access Management and (ii) the Supplier's operational Procedures as agreed with the Agency Manager and the Customer.
APPS/R/ACCMAN/002	The Supplier shall provide appropriate access (including remote access) to the necessary tools and systems to the Agency Manager, thereby enabling the Agency Manager to comply with its responsibility and obligations under its agreement with the Customer.
APPS/R/ACCMAN/003	The Supplier shall reject any access request that has not been properly approved by Agency Manager in accordance with the Access Management Policy.
APPS/R/ACCMAN/004	The Supplier shall inform the Agency Manager and the Customer where it suspects or has reason to believe that inappropriate User access has been requested.
APPS/R/ACCMAN/005	The Supplier shall assist and co-operate with the Agency Manager by granting appropriate access to Related Suppliers to the Supplier System, as applicable.

2 SERVICE DESIGN

2.1 Availability Management

Reference ID	Requirement
APPS/R/AVAMAN/001	The Supplier shall design and document the solution to be highly resilient to make the Services available to the Customer whenever possible, normally 24 hours a day, 7 days a week. It is for this reason that the Supplier shall incorporate a high degree of resilience, including, but not limited to, full mirroring of Critical Business Systems, together with well defined fail-over arrangements, thus ensuring that these systems will remain available.
APPS/R/AVAMAN/002	The Supplier shall design their services such that the duration of any necessary service withdrawal events will be kept to the absolute minimum.
APPS/R/AVAMAN/003	The Supplier shall strictly manage all proposed service withdrawals, both during Implementation and after each Operational Service commencement, and adhere with the following requirements as a minimum: a. The Supplier shall manage all operational change in accordance with the Policies, Processes and Procedures as directed by the Customer b. The Supplier shall not withdraw any service for any reason without formal Approval by the Customer. c. The Supplier shall operate on the principle of conducting all service withdrawals during periods when usage monitoring demonstrates they are least utilised over a 24 hour period. d. The Supplier shall operate with the intention of adhering to pre-defined “windows” of planned maintenance/release opportunities throughout the calendar year, to be agreed prior to Service commencement. e. The Supplier shall produce a forward plan of all planned change activity impacting availability of services on a rolling 3 month basis. f. The Supplier shall notify all Planned Service Outage to the Customer in accordance with SL’s in Call Off Schedule 6 (Service Levels, Service Credits and Performance Monitoring). g. The Supplier shall notify all unplanned service withdrawals, or emergency withdrawals which are necessary in order to resolve Incidents, in accordance with the Policies, Processes and Procedures as directed by the Customer.

2.2 Capacity Management

Background / Scope: The purpose of the Capacity Management Service is to ensure that there is sufficient capacity to enable delivery of Services.

The value 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 Customer.

Reference ID	Requirement
APPS/R/CAPMAN/001	The Supplier shall provide any reasonable information requested by the Agency Manager in respect of the Agency Manager overall capacity plan and support the on-going maintenance and development of such overall capacity plan.
APPS/R/CAPMAN/002	The Supplier shall monitor, analyse and report to the Agency Manager in relation to capacity volumes and trends and shall, where appropriate, act on any capacity related issues.
APPS/R/CAPMAN/003	The Supplier shall provide all such assistance as reasonably requested by the Agency Manager in establishing future capacity requirements for Supplier Systems, based on the Customer's defined business needs and plans. The Supplier shall make recommendations to the Agency Manager regarding how existing capacity plans for the Services are or may be affected by demand projections, and such recommendations shall include the steps needed to meet demand projections.
APPS/R/CAPMAN/004	NOT USED.
APPS/R/CAPMAN/005	The Supplier shall provide standard Service Reports which enable continual monitoring and insight into capacity trends. The Supplier shall review these reports and shall provide a dedicated Customer Support Manager to review capacity management on a monthly basis in liaison with the Supplier's technical resources.
APPS/R/CAPMAN/006	The Supplier shall manage, control and predict the performance and capacity of Operational Services. This includes initiating proactive and reactive action to address current and future performance and capacity impact of the Operational Services.
APPS/R/CAPMAN/007	The Supplier shall manage, control and predict the performance, utilization and capacity of IT resources and individual IT components (at a level to be agreed during Implementation).

3 SERVICE IMPLEMENTATION

3.1 Change Management

Background / Scope: The purpose of the Change Management Service is to identify, control and account for service assets and Configuration Items (CI's), and protect and ensure the integrity of such service assets and Configuration Items across the lifecycle of the Services.

During the Call Off Contract Period of this Call Off Contract it is anticipated that changes may be required in the delivery of the Services. Change Requests will be submitted for all proposed changes to Service, function or Service infrastructure that will or may result in:

- changes to the Call Off Contract Charges;
- changes to the scope of Service (for example, amended or new requirements);
- changes to Service Levels;
- changes to timescale
- changes in the Customer's working practices
- changes to the Call Off Contract;
- changes of any named Sub-Contractor
- changes to operational infrastructure
- other items as may be reasonably agreed from time to time.

Reference ID	Requirement
APPS/R/CHAMAN/001	The Supplier shall adhere to the Change Control Procedures as set out in Call Off Schedule 14 (Change Control Procedure)
APPS/R/CHAMAN/002	The Supplier shall contribute to the Change material in Call Off Schedule 14 (Change Control Procedure) and issue this to the Agency Manager and the Customer.
APPS/R/CHAMAN/003	The Supplier shall produce an Apps and Hosting Release Schedule and associated Release Plan(s) and issue these to the Agency Manager and the Customer. The Release Schedule will provide details for at least a three month rolling period.
APPS/R/CHAMAN/004	The Supplier shall ensure that vendor recommended patching is applied to all Assets and Software used to deliver the Services under this Call Off Contract, as directed by Agency Manager.
APPS/R/CHAMAN/005	The Supplier shall schedule, coordinate and manage Planned Service Outages in accordance with Policies, Processes and Procedures and as directed by the Customer.
APPS/R/CHAMAN/006	The Supplier shall support and assist the Agency Manager by responding to Impact Assessments and shall provide input where required.
APPS/R/CHAMAN/007	The Supplier shall monitor, analyse and report to the Agency Manager in respect of Change volumes and trends. The format of such reports shall be agreed during Implementation.
APPS/R/CHAMAN/008	The Supplier shall provide all reasonably requested Management Information to the Agency Manager
APPS/R/CHAMAN/009	The Supplier shall raise Change Requests in order to make operational or technical Changes to the Services.

Reference ID	Requirement
APPS/R/CHAMAN/010	The Supplier shall: • attend the Change Advisory Board (CAB) (including emergency CABs as necessary); • ensure that any issues related to the Supplier raised at the Change Advisory Board meeting are progressed to the satisfaction of Agency Manager; and • where required by the Agency Manager, provide such support reasonably requested to enable the progression of changes owned by Other Suppliers. The Supplier retains the right to request that Project work relating to Other Supplier change may be the subject of a Change Request.
APPS/R/CHAMAN/011	The Supplier shall track and monitor all approved Changes and ensures that Change records are updated throughout the lifecycle of each Change in accordance with decisions made at the Change Advisory Board.
APPS/R/CHAMAN/012	The Supplier shall ensure that operational change requests contain information including, but not limited to: (i) Implementation Plans; (ii) Test Success Criteria; (iii) Back Out Plans or Remediation Plans; (iv) Plans for handover to support; (v) User communication plans; and (vi) Configuration Items affected.
APPS/R/CHAMAN/013	Following implementation of an operational change, the Supplier shall ensure that Post Implementation Reviews implemented by Agency Manager are carried out and managed effectively, and that any lessons learned from each Post Implementation Review are implemented and fed into the assessment of future Changes.
APPS/R/CHAMAN/014	The Supplier shall ensure that any operational changes that occur more often than three (3) times each rolling monthly period are processed consistently with the requirements of the Agency Manager.
APPS/R/CHAMAN/015	The Supplier shall ensure that all pre-approved Changes are publicised by the Agency Manager in the Service Catalogue.
APPS/R/CHAMAN/016	The Supplier shall: (i) identify any potential Change Management process improvements; (ii) make appropriate recommendations to the Agency Manager; and (iii) where these are agreed by the Customer, the Supplier shall manage any process improvement activity until completed.
APPS/R/CHAMAN/017	The Supplier shall adhere to the governance required by the

Reference ID	Requirement
	Agency Manager and/or the Customer regarding Change Requests, including): (i) the raising and recording of Changes; (ii) the assessment and evaluation of the Change; (iii) the cost and the benefit of the proposed Change; and (iv) the review and closure of Changes .
APPS/R/CHAMAN/018	In respect of Change, the Supplier shall ensure that all Assets used in delivering the Services adhere at all times to; (i) any hardware vendor support requirements; and (ii) any requirements of the Agency Manager relating to Incident Management.
APPS/R/CHAMAN/019	The Supplier shall: (i) ensure that any compatibility issues between the Customer's Systems immediately prior to the Call Off Commencement Date and new or proposed Supplier Systems are identified as soon as reasonably practicable and in any event prior to the date of Achievement of the relevant Operational Services Commencement Date; and (ii) assist and co-operate with the Agency Manager to determine the treatment of such compatibility issues.
APPS/R/CHAMAN/020	NOT USED.
APPS/R/CHAMAN/021	NOT USED.

3.2 Software Asset and Configuration Management (SACM)

Reference ID	Requirement
APPS/R/SACM/001	The Supplier shall maintain accurate Asset details, including details of the hardware, operating system and any bespoke or packaged Software in order for the Agency Manager to maintain the CMDB.
APPS/R/SACM/002	The Supplier shall where necessary carry out Asset disposal; including the procurement of formal certification that secure and environmentally responsible disposal has been conducted, and shall notify the Agency Manager of such disposals, in order for the Agency Manger to maintain the CMDB.
APPS/R/SACM/003	The Supplier shall agree and provide regular reporting to the Agency Manager and the Customer regarding any relevant licence compliance for all Software provided by the Supplier used to deliver the Supplier Solution.

Reference ID	Requirement
	For all Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.
APPS/R/SACM/004	The Supplier shall work with the Agency Manager and the Customer, as reasonably required, to confirm the scope of any Asset Management audits and the investigation and resolution of any discrepancies related to Asset Management. Unless agreed otherwise by the Parties, such Asset Management audits shall occur at least once per year during the Call Off Contract Period, at no additional Charge to the Customer.
APPS/R/SACM/005	The Supplier shall provide the results of Asset Management audit data to the Agency Manager within the timescales and in the format reasonably required by the Agency Manager.
APPS/R/SACM/006	The Supplier shall receive, review and, when instructed by the Agency Manager and/or the Customer implement recommendations for Service Asset and Configuration Management process improvements. If the scale and nature of these improvements requires additional resources, this may be subject to agreement under the Change Control Procedure.
APPS/R/SACM/007	The Supplier shall provide CI (Configuration Item) data to the Agency Manager in a format and frequency appropriate for inclusion in the Agency Manager supplied integrated CMDB.
APPS/R/SACM/008	The Supplier shall develop, test and implement changes to asset management system interfaces and Configuration Item data content as agreed with the Agency Manager. If the scale and nature of these changes requires additional resources this may be subject to agreement under the Change Control Procedure.
APPS/R/SACM/009	The Supplier shall assist and co-operate with the Agency Manager in determining the reason for each Configuration Item discrepancy, its criticality, and actions required to address it.

3.3 Knowledge Management

Reference ID	Requirement
APPS/R/KNOWM/001	The Supplier shall contribute to the knowledge management system provided by the Agency Manager for the capture, storage, and presentation of information required to manage the

Reference ID	Requirement
	Services.
APPS/R/KNOWM/002	The Supplier shall ensure that, where data created by the Supplier is found in the knowledge management system provided by the Agency Manager that is inaccurate, incomplete or lacks integrity, such data is promptly corrected.
APPS/R/KNOWM/003	The Supplier shall assist and co-operate with the Agency Manager in ensuring the knowledge management system contains data and information, including: i. methods to resolve Incidents; ii Known Errors; iii. Service Desk scripts; iv. build data; v. self-help articles; and vi. frequently asked questions (FAQs).

3.4 Service Implementation

Reference ID	Requirement
APPS/R/SERVTRA/001	The Supplier shall ensure that the Implementation phase does not interrupt normal operations and availability unless absolutely necessary and, where necessary, should follow the Change Process Policies, Processes and Procedures as directed by the Customer.
APPS/R/SERVTRA/002	The Supplier shall define the data migration approach in the Supplier's Implementation Plan.
APPS/R/SERVTRA/003	User profiles and associated data shall be migrated in a planned and verifiable manner with no loss of data or data integrity.
APPS/R/SERVTRA/004	The Supplier shall ensure that backups can be recovered from the pre-migrated system to the new system once migration has taken place.
APPS/R/SERVTRA/005	The Supplier shall provide a roll back plan as part of each operational change request raised, to mitigate for any issues during transition to the new hardware and software.
APPS/R/SERVTRA/006	The Supplier shall ensure that there are sufficient dry-runs to validate the Data Migration, Cutover and Rollback procedures. The Supplier shall ensure that the disaster recovery environment is available prior to cutover to the Supplier Solution.
APPS/R/SERVTRA/007	Supplier passwords for all applications and systems supported by the Supplier to be reset (where possible remotely) by the Supplier (i) as required by the Agency Manager; or (ii) provided that, if the Supplier is resetting passwords, it will follow the process set out in the SOM.

4. I.T. SERVICE CONTINUITY MANAGEMENT (ITSCM)

Reference ID	Requirement
APPS/R/ITSCM/001	The Supplier shall make sure that all Supplier Personnel with responsibilities for fighting disasters are aware of their exact duties, and to make sure that all relevant information is readily available when a disaster occurs.
APPS/R/ITSCM/002	The Supplier shall design appropriate and cost-justifiable continuity mechanisms and procedures to meet the Business Continuity Plan and Disaster Recovery Plan as set out in Call Off Schedule 10 (Business Continuity and Disaster Recovery). This includes the design of risk reduction measures and recovery plans.
APPS/R/ITSCM/003	The Supplier shall ensure preventive measures and recovery mechanisms for disaster events are subject to regular testing.
APPS/R/ITSCM/004	The Supplier shall create and make available to the Customer detailed instructions on when and how the Supplier will invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first steps to be taken by the Supplier upon learning that a (suspected) disaster has occurred.

5. SERVICE DESIGN

5.1 Service Catalogue Management

Reference ID	Requirement
APPS/R/SCM/001	The Supplier shall contribute to and use the Business Service Catalogue.
APPS/R/SCM/002	The Supplier shall provide a Service Catalogue, containing all commodity products to be provided by this Supplier. Service Catalogue pro-forma to be agreed during Implementation
APPS/R/SCM/003	The Supplier shall review Management Information on a monthly basis to identify trends or significant changes or increases in service request volumes, for discussion with the Agency Manager and, where necessary, Related Suppliers, as applicable.
APPS/R/SCM/004	The Supplier shall identify possible Process improvements and promptly make appropriate recommendations to the Agency Manager in writing.
APPS/R/SCM/005	The Supplier shall immediately bring to the attention of the Agency Manager any issues that prevent the Supplier from processing Service Requests.
APPS/R/SCM/006	The Supplier shall ensure that Service Requests received from the Agency Manager are expedited within agreed Service Levels when assigned by the Service Desk

Reference ID	Requirement
APPS/R/SCM/007	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Agency Manager in response to Service Requests.
APPS/R/SCM/008	The Supplier shall: (i) co-operate with the Agency Manager to proactively manage and monitor the status and progress of all Service Requests for the Services ordered via the Business Service Catalogue; and (ii) adhere to the PPP relevant to Service Requests as provided by the Agency Manager.
APPS/R/SCM/009	The Supplier shall respond to the Agency Manager or the Customer's enquiries regarding Service Requests with accurate and up-to date information.
APPS/R/SCM/010	The Supplier shall manage end of life Service Catalogue items, such that, at least one month before the end of life Service Catalogue item is discontinued, replacement Service Catalogue items: a. are adequately tested (including User acceptance testing where appropriate); b. are Approved by the Customer; c. have any relevant Call Off Contract Charges agreed between the Supplier and Customer; d. added to the Service Catalogue; and e. any relevant Test Environment(s) is created.

5.2 Service Level Management

Reference ID	Requirement
APPS/R/SLM/001	NOT USED.
APPS/R/SLM/002	NOT USED.
APPS/R/SLM/003	NOT USED.
APPS/R/SLM/004	NOT USED.
APPS/R/SLM/005	NOT USED.
APPS/R/SLM/006	The Supplier to provide a monthly Performance Monitoring Report, and within this report to compare the agreed and actually Achieved Service Levels, and also include information on the usage of services, ongoing measures for service improvement, and any exceptional events that occurred during the period measured.

Reference ID	Requirement

6. CONTINUAL SERVICE IMPROVEMENT

Reference ID	Requirement
APPS/R/CSI/001	The Supplier shall review all of the services provided by the Supplier on a regular basis, with a view to improving service quality where necessary, and to identify more economical ways of providing a service where possible.
APPS/R/CSI/002	The Supplier shall evaluate processes on a regular basis. Such evaluation to include identifying areas where the targeted process metrics are not reached, holding regular benchmarkings, audits, maturity assessments and reviews.
APPS/R/CSI/003	The Supplier shall define specific initiatives aimed at improving services and processes, based on the results of service reviews and process evaluations. The resulting initiatives shall either be internal initiatives pursued by the Supplier on its own behalf, or initiatives which require the Customer's cooperation.
APPS/R/CSI/004	The Supplier shall verify if improvement initiatives are proceeding according to plan, and introduce corrective measures where necessary.

ANNEX 1 OF PART A – STRUCTURAL REQUIREMENTS FOR CMS, WMS AND MIS

In relation to the CMS, WMS and MIS applications, the purpose of this Annex is to list (i) the referenced documents in Part A and (ii) background and overview documentation.

TABLE 1: COMPASS Overview

Description	Document
Outline Design Specifications	253020 (5.50) COMPASS Outline Design Spec
Asset register – COMPASS programme	CD000_Compass Document Asset Register 20170612 V1.0
Overall Design specification – COMPASS programme	CD037_253020 (5.50) ods
Overview of Customer products	CD048_REDACTED_353709 overview of CPS products 2014R3
Software assets	CD146_CPS Software List External 20170522 Data Room
Hardware assets	CD187_CGI CMDB hardware asset list 24-May-2017 v1 2

TABLE 2: CMS overview and Functional Specifications (includes details of WMS and MIS)

Description	Document
User requirements for the changes to CMS, WMS and MIS implemented by Supplier for Release 3 of CMS 2014.	CD009_107054906 - CMS 2014 R3 Consolidated v1.0 (NB This is an typical example of an agreed user requirement for a specific release of CMS provided by the Former Supplier)
Hardware Infrastructure for CMS	CD010_REDACTED_900805-003 (2.0) CMS DCTR 2013 Hardware TDS
Software Infrastructure for CMS	CD011_REDACTED_900802-001 (1.0) CMS DCTR 2013 Software TDS
CMS High Level Design Specification	CD012_502001-001 (2.00) CMS High Level Design Specification
Functional Specification: document contents page	CD064_453001_00 (18.00) CMS FS Front Material
Functional Specification section 1: brief overview of the CMS and WMS	CD065_453001_01 (18.00) CMS FS Management Summary
Functional Specification section 2: a more detailed introduction to the CMS and WMS.	CD066_REDACTED_453001_02 (18.00) CMS FS Introduction
Functional specification section 3: the Business Context	CD067_453001_03 (18.00) CMS FS Business Context
Functional specification section 4: functional overview	CD068_453001_04 (18.00) CMS FS Functional Overview
Functional specification sections 5-12: subsystems	See tables 3, 4 and 5 below.

Functional specification section 13: data requirements	CD109_453001_13 (18.00) CMS FS Data Requirements
Functional specification section 14: user interface	CD110_453001_14 (18.00) CMS FS User Interface Requirements
Functional specification section 15: Non Functional requirements	CD111_453001_15 (18.00) CMS FS Non-functional Requirements
Functional specification, Appendix A: glossary	CD112_453001_A (18.00) CMS FS Glossary
Functional specification, Appendix B: Screen Layout	See tables 3 and 4
Functional specification, Appendix C: Logical data model	CD127_453001_C (18.00) CMS FS Logical Data Model
Functional specification, Appendix D: User Style Guide	453001_D (18.00) CMS FS User Interface Style Guide
Functional specification, Appendix E: Interface specifications	CD129_453001_E (18.00) CMS FS External Interfaces
Functional specification, Appendix F: Function mapping	CD130_453001_G (18.00) Cat Item Mapping
Functional specification, Appendix G: System Generated Outputs Layout	CD131_453001_G (18.00) CMS FS Generated Outputs CD132_453001_G (18.00) WMS FS Generated Outputs
Functional specification, Appendix	CD133_453001_H (18.00) CMS FS Print Views CD134_453001_H (18.00) WMS FS Print Views

TABLE 3: CMS Sub-Systems Functional Specifications

Sub-System	Sub-Sections	Document(s)
Cases (C)	General Case Facilities (CG1/2)	CD087_453001_08_CG1 (18.00) CMS FS Cases subsystem CD088_453001_08_CG2 (18.00) CMS FS Cases subsystem
	Case Allocation (CA)	CD079_453001_08_CA (18.00) CMS FS Cases subsystem
	Structured Bundling (CB)	CD080_453001_08_CB (18.00) CMS FS Cases Bundles
	Counts and Indictments Preparation (CC)	CD082_453001_08_CC (18.00) CMS FS Cases subsystem
	Case Pre-Charge Decision (CD)	CD083_453001_08_CD (18.00) CMS FS Cases subsystem
	Case Progression Functionality (CE)	CD085_453001_08_CE (18.00) CMS FS Cases subsystem
	Confiscation Cases (CF)	CD086_453001_08_CF (18.00) CMS FS Cases subsystem
	Output Production (CO)	CD089_453001_08_CO (18.00) CMS FS Cases subsystem
	Hearing Preparation	CD090_453001_08_CP (18.00) CMS FS Cases

	(CP)	subsystem
	Case Review (CR)	CD091_453001_08_CR (18.00) CMS FS Cases subsystem
	Case Transfer (CT)	CD092_453001_08_CT (18.00) CMS FS Cases subsystem
	Victim Code Communications (VC)	CD093_453001_08_VC (18.00) CMS FS Cases subsystem
Hearings Subsystem (H) – CMS	Record Hearings (RH) Split and Merge (HS)	CD101_453001_09 (18.00) CMS FS Hearings Subsystem
Materials (M)	Register Case (MR)	CD077_453001_07_MR (18.00) CMS FS Material Subsystem
	Electronic Receipt of Unstructured Material (MU)	CD078_453001_07_MU (18.00) CMS FS Material Subsystem
	Electronic Receipt of Structured Material (ME)	CD075_453001_07_ME (18.00) CMS FS Material Subsystem
	Electronic Receipt of Structured Material from PROGRESS (MP)	CD076_453001_07_MP (18.00) CMS FS Material Subsystem
	CMS Material Archiving (MA)	CD074_453001_07_MA (18.00) CMS FS Material Subsystem
Control (L)	Tasks (LT)	CD069_453001_05 (18.00) CMS FS Control subsystem
	User Access (LU)	
	Control Rule Set (LC)	
	Menus and Navigation (LM)	
Monitor (T)	Manage Monitoring (TM)	CD071_453001_06 (18.00) CMS FS Monitor Subsystem
Report (R)	Reports View (WRV) &	CD103_453001_10 (18.00) CMS FS Report Subsystem
	Report Production (WRP)	
Configuration (F)	Static Data (FD)	CD105_453001_11 (18.00) CMS FS Configuration Subsystem
	Security (FS)	
Support (S)	Electronic Document Handling (SD)	CD107_453001_12 (18.00) CMS FS Support Subsystem
	Audit Trail (SA)	
	Find Cases (SF)	
	Legacy Cases (SL)	
	External Interfaces (SI)	
(Various)	Screen layout	CD113_453001_B (18.00) CMS FS Case Subsystem Screen Layout CD114_453001_B (18.00) CMS FS Configuration Subsystem Screen Layout CD115_453001_B (18.00) CMS FS Control Subsystem Screen Layout CD116_453001_B (18.00) CMS FS Hearings

		Subsystem Screen Layout CD117_453001_B (18.00) CMS FS Material Subsystem Screen Layout CD118_453001_B (18.00) CMS FS Report Subsystem Screen Layout CD119_453001_B (18.00) CMS FS Support Subsystem Screen Layout

TABLE 4 - WMS Sub-Systems Functional Specifications

Sub-System	Sub-Sections	Document(s)
Cases (WC)	General Case Facilities (WCG)	CD096_453001_08_WCG1 (18.00) WMS FS Case subsystem CD097_453001_08_WCG2 (18.00) WMS FS Case subsystem
	Case Allocation (WCA)	CD094_453001_08_WCA (18.00) WMS FS Cases subsystem
	WMS Case Progression Functionality (WCE)	CD095_453001_08_WCE (18.00) WMS FS Cases subsystem
	Output Production (WCO)	CD098_453001_08_WCO (18.00) WMS FS Cases subsystem
	Hearing Preparation (CP)	CD090_453001_08_CP (18.00) CMS FS Cases subsystem
	Case Transfer (WCT)	CD099_453001_08_WCT (18.00) WMS FS Cases subsystem
	WMS Victim Code Functionality (WVC)	CD100_453001_08_WVC (18.00) WMS FS Cases subsystem
Hearings Subsystem (H)		CD102_453001_09 (18.00) WMS FS Hearings Subsystem
Control (WL)	Tasks (WLT)	CD070_453001_05 (18.00) WMS FS Control subsystem
	User Access (WLU)	
	Menus and Navigation (WLM)	
	Case Locking (WLK)	
Monitor (WT)	Manage Monitoring (WTM)	CD072_453001_06 (18.00) WMS FS Monitor Subsystem
Report (WR)	Reports View	CD104_453001_10 (18.00) WMS FS Report

	(WRV) & Report Production (WRP)	Subsystem
Configuration (WF)	Static Data (WFD) Security (WFS)	CD106_453001_11 (18.00) WMS FS Configuration Subsystem
Support (WS)	Audit Trail (WSA) Find Cases (WSF)	CD108_453001_12 (18.00) WMS FS Support Subsystem
Material (WM)		CD073_453001_07 (18.00) WMS FS Material Subsystem
(Applicable to all subsystems)	Screen Layout	CD120_453001_B(W) (18.00) WMS FS Case Subsystem Screen Layout; CD121_453001_B(W) (18.00) WMS FS Configuration Subsystem Screen Layout CD122_453001_B(W) (18.00) WMS FS Control Subsystem Screen Layout; CD123_453001_B(W) (18.00) WMS FS Hearings Subsystem Screen Layout; CD124_453001_B(W) (18.00) WMS FS Material Subsystem Screen Layout CD125_453001_B(W) (18.00) WMS FS Report Subsystem Screen Layout; CD126_453001_B(W) (18.00) WMS FS Support Subsystem Screen Layout
No subsystem reference	WMS Master Task List	CD136_453013 WMS master task list (FS v18.00)

TABLE 5: MIS Functional Specifications

Sub-System	Sub-Sections	Document(s)
N/A	N/A	CD034_553001 (13.00) MIS Functional Specification CD034_553001 (13.00) MIS Functional Specification - Reports CD034_553001 (13.00) MIS Functional Specification - Appendices CD033_REDACTED_553201 (12.06 working) (R7.0.07.B) Extract Module Specification

TABLE 6: EMS and other systems

System	Document(s)
EMS	CD192_REDACTED_EMS High Level Design v1.0 CD193_REDACTED_EMS Top Level Design v0 30

Prosecutor App	CD188_REDACTED_7081_CGI_CPS App_FS_v1_4 CD189_REDACTED_7081_CGI_CPSAppDelivery_TechSpec_v1_1
Sharepoint	The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000
BES	
Email (websense)	
Remote Access (Juniper)	
Solidus	
SCCM	

TABLE 7 – Policies and related documents

CD061_Managing catalogues and requests v0.9 AMA
CD152_REDACTED_CPS OFD - Issued V1.0
CD153_REDACTED_CPS Service Operations - Availability and Capacity Policy V1.0
CD156_REDACTED_CPS Service Operations - Change and Release Management Policy v1.0
CD160_REDACTED_CPS Service Operations - Incident Management Policy v1.0
CD162_REDACTED_CPS Service Operations - Knowledge Management Policy and Process V1.0
CD164_REDACTED_CPS Service Operations - Problem Management Policy v1.0
CD167_REDACTED_CPS Service Operations - SACM Policy v1.0
CD169_REDACTED_Service Catalogue Management-PP V1.0 shared with Suppliers 25.01
CD170_REDACTED_CPS Service Operations - Service Level Management Policy v1.0
CD172_REDACTED_CPS Service Operations - Service Reporting Policy v1.0
CD174_REDACTED_CPS Service Operations - Service Request Management Policy v1.0
CD176_REDACTED_CPS Service Operations - Supplier Management Policy V1.0
CD177_REDACTED_CPS Service Operations - Transition Planning and Support Policy and Process V1.0A
CD191_Managing CCRs v1 10

TABLE 8 – Architecture, Design and Interfaces

CD015_REDACTED_25.16.03 Compass Office Architecture (3.10)
CD036_REDACTED_NWNJ Technical Architecture
CD150_253022 (0.2) Architecture Target
CD151_253022 (0.2) Architecture Baseline
CD013_1038301 Colmore Gate High Level Design (0.3)
CD021_REDACTED_522010 CPSD Detailed Design (1.0)_
CD022_82500701 (2.0) CPSD High Level Design
CD024_1038201 Drummond Gate High Level Design (2.0)
CD035_1021009 Network Backup High Level Design (v0.11)

CD140_REDACTED_103.31.11.21 (1.2) RCI Office Host Server Build
CD141_REDACTED_103.31.11.22 (1.1) RCI Satellite Server Build
CD142_REDACTED_103-31-81-10-03 Rose Court Server Detailed Design V1 06
CD143_REDACTED_CPS Drummond Gate Office Server Detailed Design (2.0) Issued
CD144_REDACTED_103-31-83-02 CPS Colmore Gate Server Detailed Design (1.0)
CD145_REDACTED_103-31-84-02 CPS Manchester Server Detailed Design 1.0
CD178_REDACTED_82660801 EUDR High Level Design (1.1)
107 05 72 06 04 CMS to C2I DX Functional Design v1 4
25501706 (1.00) Police XML Interface Business Process Document
50404010 CMS API Interface Control Document (2 02)
CD019_REDACTED_1150701 CPS PNC Access Technical Specification (1.1)

TABLE 9 – Other COMPASS documents

Topic	Document(s)
CPS website	CD020_REDACTED_9936-002 Internet 2nd Line Support Procedure v3.4
IT and Telephony Services	CD041_REDACTED_Business Service Catalogue v4.0
Monitoring(?)	CD030_REDACTED_6615100-001 (0.02) D-and-I Live System Monitoring
Risk	CD190_REDACTED_172505-1_RMADS_V19_0 v10
Call volumes	CD194 CPS Tickets - call volumes Dec16-May17 v0.3
PSN	CD025_REDACTED_82.68.08.01 GCF to PSN transition v1.00(draft)
Xerox	CD181_Xerox CMPS hosting High Level Design (1.0)
	CD135_453013 master task list (FS v18.00)
	CD180_REDACTED_103313401 RCI Packet Shaper design v4.1
	CPS proposed Non Functional test criteria v1.0
	CPS_Validation_Diagram_V15

TABLE 10 – other documents referenced in this Call Off Schedule

The Customer's digital strategy	CPS Digital Strategy 2020 Final.PDF – see VDR
The Customer's cloud security strategy	CPS Cloud Security Strategy v1.1 – see VDR
The Customer's Annual Report and Accounts.	See www.cps.gov.uk
HMCTS Court Store system, described in document reference <HMCTS Court Store ICD 113.doc>	Will be made available on Implementation
Introduction to the CPP	https://insidehmcts.blog.gov.uk/2016/06/30/introduction-to-common-platform-programme/
The Customer's current	https://www.cps.gov.uk/cymraeg/assets/uploads/files/CYNLLU

Welsh language scheme	N%20IAITH%20GYMRAEG%20-%20WELSH%20LANGUAGE%20SCHEME.pdf.

ANNEX 2 OF PART A – LIST OF SHAREPOINT APPLICATIONS

#	Application Name
1	**ADV Assessments**
2	**Appellate Court List**
3	**BIS Gateway in ICT SC**
4	**CAD Web App Home Page**
5	**Call Log**
6	**Casework Quality**
7	**CCTRS - Complex Casework Time Recording**
8	**Change Unit Communications**
9	**CJSM_List**
10	**CPS Diversity Champion Forum in EDU**
11	**CTL Discrepancy**
12	**Discipline and Grievance**
13	**East Mids Community Engagement**
14	**eForms**
15	**ePDR**
16	**F2F Training - Course Selection**
17	**Facility Time in HR**
18	**ILA London**
19	**IQA in the OP site collection**
20	**Liaisons**
21	**London Charging Diary**
22	**London Meeting Room Booking App**
23	**MAP Desk**
24	**MMR**
25	**My HR**
26	**NBCPA Application Form**
27	**New Area Liaison Site**
28	**Overpayments Register**
29	**PAPPI in the ICT SC**
30	**Pay and Benefits in HR**
31	**PEFORM App**
32	**PQ & MP Correspondence Apps**
33	**Recognition Hub within HR**

#	Application Name
34	**REM Home**
35	**Sensitive Cases**
36	**Service Catalogue (Being built)**
37	**Shift Report V2**
38	**South East Meeting Room Manager**
39	**South West Leave Data**
40	**South West Monitoring**
41	**South West Travel and Expenses**
42	**South West Triage PCD process data**
43	**Staff Awards**
44	**Thames & Chiltern Community Engagement**
45	**Trace**
46	**TRACE Archive**
47	**VHCC Fees**
48	**VRR**
49	**Wessex - Building Issues Log**
50	**West Midlands Community Engagement**
51	**Workplace Adjustment Passport**
52	**Yorks & Humber Community Engagement and Equality & Diversity**

PART B: SUPPLIER SERVICE DESCRIPTIONS

1.1. This Part B describes how the Supplier Solution shall comply with all of the Service Requirements set out in Part A of this Call Off Schedule.

1.2. The Supplier shall provide the Services without any disruption to the Customer and its Users, save as otherwise set out in the Call Off Contract or as agreed in the PPP's.

1.3. The Supplier shall supply the Services to meet the Customer's Service Requirements.

1.4. A summary of the Supplier Solution is set out below under this Paragraph 1.4.

The Solution Overview

The Supplier Solution meets the Customer needs and can be achieved and meets the Service Requirements set out in this Call Off Schedule 2 Part A as well as the services functions, requirements, responsibilities and/or deliverables for the Call Off Schedule 14 (Change Control Procedure), Call Off Schedule 8 (Security), Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel) and Call Off Schedule 10 (Business Continuity and Disaster Recovery).

The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000

CATEGORY 1: GENERAL REQUIREMENTS

#	Requirement	Supplier Response
APPS/R/GREQ/001	The Supplier shall deliver all Services in accordance with the Call Off Terms of the Call Off Contract, including the Standards.	The Supplier is compliant with this Requirement. The Supplier shall deliver all Services in accordance with the Call Off Terms of the Call Off Contract, including the Standards.
APPS/R/GREQ/002	The Supplier shall, wherever possible, use Standards-based solutions. This shall apply to technical solutions as well as management and operational interactions between the Supplier and the Agency Manager (e.g., operating models based on COBIT (Control Objectives for Information and Related Technology), TOGAF (The Open Group Architecture Framework), and ITIL (Information Technology Infrastructure Library)).	The Supplier is compliant with this Requirement. The Standards to be used will be defined in the SOM.
APPS/R/GREQ/003	To ensure that maximum process efficiency and data quality are obtained in relation to the Services, the Services shall be automated by the Supplier wherever there is the opportunity to do so. The Supplier shall ensure that the Services shall be designed to capture data only once, thus minimising the need for manual data capture and input. All data shall be validated by the Supplier on input.	The Supplier is compliant with this Requirement.
APPS/R/GREQ/004	The Supplier shall wherever possible use simplified assurance and payment processes when invoicing the Customer.	The Supplier is compliant with this Requirement. The Supplier shall follow the invoicing processes defined in Paragraph 16 of Call Off Schedule 3 (Call Off Contract

#	Requirement	Supplier Response
		Charges, Payment and Invoicing).
APPS/R/GREQ/005	Save as otherwise expressly stated in the Call Off Contract, the Supplier shall ensure that, upon request from the Customer, certain of: (i) the Supplier's Personnel; (ii) and any of the Key Personnel; and/or (iii) other relevant persons identified by the Customer that the Customer wishes to meet, shall attend workshops or meetings with the Customer and/or any other Related Supplier as the Customer reasonably deems necessary given the circumstances.	The Supplier is compliant with this Requirement. The Supplier will attend workshops and meetings in accordance with the provisions of Call Off Schedule 17 (Governance).
APPS/R/GREQ/006	Where the Supplier fails, or becomes aware that it is likely to fail to comply with any obligation of this Call Off Contract and such failure may impact on the performance of the Services by the Supplier (including the Service Levels), the Supplier shall, as soon as is reasonably practicable, notify the Customer of such failure or likely failure.	The Supplier is compliant with this Requirement. The Supplier will notify the Customer in accordance with a process to be defined and agreed in the SOM.
APPS/R/GREQ/007	The Supplier shall notify the Customer when it becomes aware of an actual or potential event that may pose a risk to the Services and shall provide to the Customer all necessary details and information of such event.	The Supplier is compliant with this Requirement. The Supplier will notify the Customer in accordance with a process to be defined and agreed in the SOM**.**
APPS/R/GREQ/008	The Supplier shall comply with the Data Protection Legislation and data protection provisions set out in the Call Off Contract, including in relation to the Processing of the Personal Data controlled by the Customer.	The Supplier is compliant with this Requirement. The Supplier will perform its obligations in accordance with Clause 35.7 of the Call Off Terms and Call Off Schedule 8 (Security).

#	Requirement	Supplier Response
APPS/R/GREQ/009	The Supplier shall provide support to the Related Suppliers including, where necessary, access to resources, the Supplier System, Software and any materials as required, and to deal with security and/or compliance issues, assessments and actions. Any work arising under this requirement that is outside the scope of the PPPs would be subject to Call Off Schedule 14 (Change Control Procedure).	The Supplier is compliant with this Requirement.
APPS/R/GREQ/010	The Supplier shall perform the Services in accordance with Clause 7/8 of the Call Off Terms and this Call Off Schedule. The Supplier shall use ITIL (Edition 2011 or the then current version of ITIL) based processes and perform the Services in accordance with industry based best practice and, if required, the Supplier shall demonstrate this to the satisfaction of the Customer.	The Supplier is compliant with this Requirement. The Supplier will perform the Services in accordance with a process to be defined and agreed in the SOM.
APPS/R/GREQ/011	The Supplier shall adhere to the Agency Manager provided common Standards for interfaces to the ITSM Toolset for the management of Services events across the Service Management Lifecycle. Amendments to such common Standards that result in a material change to the Supplier Solution shall be subject to Call Off Schedule 14 (Change Control Procedure).	The Supplier is compliant with this Requirement.
APPS/R/GREQ/012	The Supplier shall ensure that Processes for all ITIL functions are aligned (to the work instruction procedural level) with the Policies, Processes and Procedures set out by the Customer by the end of Implementation. The Supplier shall ensure that all hand-over and hand-back	The Supplier is compliant with this Requirement. The Supplier will perform the Services in accordance with a process to be defined and agreed in the SOM.

#	Requirement	Supplier Response
	points and Dependencies between: (i) the Supplier and the Customer, (ii) the Supplier and the Agency Manager; (ii) the Supplier and Related Suppliers are clearly set out in the SOM. Amendments to such Policies, Processes and Procedures that result in a material change to the Supplier Solution shall be subject to Call Off Schedule 14 (Change Control Procedure).	
APPS/R/GREQ/013	The Supplier Solution shall be implemented in a modular and commoditised way, allowing for flexible and scalable Services that can be updated and replaced with minimal disruption to the Customer.	The Supplier is compliant with this Requirement. The Supplier shall implement solutions in a modular and commoditised way, allowing for flexible and scalable Services that can be updated and replaced with minimal disruption to the Customer.
APPS/R/GREQ/014	The Supplier shall facilitate process efficiency by choosing automation over manual intervention and empowering the business to self-serve, subject to such automation being Approved by the Customer in advance.	The Supplier is compliant with this Requirement. The Supplier will facilitate process efficiency in the operation and development of Services. The implementation of Robotic Process Automation shall be undertaken in consultation with the Customer via the Change Control Procedure.
APPS/R/GREQ/015	The Supplier shall ensure that the Supplier Solution shall have a documented design and be implemented such that it has optimum scalability, and for process and technology integration with other Related Suppliers. Any material changes required to the Supplier Solution arising out of such process and technology integration with Related Suppliers shall be subject to Call Off Schedule 14 (Change Control Procedure).	The Supplier is compliant with this Requirement. The Supplier shall produce a documented design and the scalability offered by the Supplier shall be set out in the agreed documented design.

#	Requirement	Supplier Response
APPS/R/GREQ/016	The updating of Service event data shall occur immediately or in sufficient time to enable effective Management Information to be produced and acted upon in accordance with Service Levels, Service Level Performance Measures, and Key Performance Indicators for the Services.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GREQ/017	The Supplier shall ensure that all necessary support is provided to the Customer, or any Auditor assigned or appointed by the Customer, to audit any aspect of the Services provided by the Supplier.	The Supplier is compliant with this Requirement. The Supplier shall provide support for audit of the Services it provides.
APPS/R/GREQ/018	The Supplier shall annually assess the maturity of the Services using the HMG Green ICT Maturity Assessment Model and the Supplier shall provide the findings to the Customer within thirty (30) Working Days of each annual anniversary of the date of Achievement of the Final Operational Services Commencement Date.	The Supplier is compliant with this Requirement.
APPS/R/GREQ/019	The Supplier shall bear the cost of decommissioning, collection and disposal of Supplier Equipment.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GREQ/020	The Supplier shall provide to the Customer access for validation purposes to all raw data and access on demand to all the Supplier's reporting tools.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GREQ/021	The Supplier shall provide a SOM in accordance with Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel) and update it in consultation with the Customer from time to time and	The Supplier is compliant with this Requirement.

#	Requirement	Supplier Response
	baseline it annually on each anniversary of the Call Off Commencement Date.	
APPS/R/GREQ/022	The Supplier shall act as the operational agent on behalf of the Customer for Crown Hosting services procured by the Customer. The scope of such work shall be as set out in the applicable procurement contract with Crown Hosting which shall be agreed (such agreement not to be unreasonably withheld or delayed) in advance with the Supplier.	The Supplier is compliant with this Requirement.

CATEGORY 2: OPERATIONAL/ TECHNICAL REQUIREMENTS

1. Data Hosting

1.1 Data Hosting

Reference ID	Requirement	Supplier Response
APPS/R/HOST/001	The Supplier shall provide and support a Private or Community Cloud environment to the Customer.	The Supplier is compliant with this Requirement. The Supplier will provide a Community Cloud environment as defined by the NIST Standards.
APPS/R/HOST/002	The Supplier shall ensure data centres used in the provision of the service are registered as participants under the EU Code of Conduct for Data Centres Energy Efficiency.	The Supplier is compliant with this Requirement. The data centres used in the provision of the service are registered as participants under the EU Code of Conduct for Data Centres Energy Efficiency.
APPS/R/HOST/003	The Supplier shall provide the following infrastructure within their data centres a. Infrastructure application servers b. Database management servers c. Authentication servers d. Application servers e. Management servers f. Backup servers g. Unix servers (where required)	The Supplier is compliant with this Requirement. Servers will be provided to perform one or many of these functions as required to deliver the Services. Backup / archive may use tape libraries, or may use disk storage - that is an Implementation detail to be defined in the design.

Reference ID	Requirement	Supplier Response
	h. Data Storage for both structured and unstructured CMS data. i. Tape Library(s)	
APPS/R/HOST/004	The Supplier shall Implement, maintain and support standard physical server builds sized by CPU, number of cores, RAM and interfaces, to be offered in small, medium, and enterprise builds in support of the Services.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/005	The Supplier shall Implement, maintain and support standard virtual server builds sized by CPU, number of cores, RAM and interfaces, to be offered in small, medium, and enterprise builds in support of the Services.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/006	The Supplier shall provide connectivity into the Customer WAN cloud and external networks such as the CJX and PSN networks.	The Supplier is compliant with this Requirement.
APPS/R/HOST/007	The Supplier shall provide fail over resilience between data centres.	The Supplier is compliant with this Requirement. See response to APPS/R/HOST/014. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/008	The Supplier shall provide backup and recovery to tape and disk storage.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further

Reference ID	Requirement	Supplier Response
		information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/009	The Supplier shall provide resilient power to all data centre hosted servers and infrastructure equipment.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/010	The Supplier shall provide management information & monitoring of all servers.	The Supplier is compliant with this Requirement. The Supplier will use monitoring, alerting and reporting toolsets.
APPS/R/HOST/011	NOT USED.	NOT USED
APPS/R/HOST/012	The Supplier shall provide the ability to offload files, media, images and other agreed objects from compute resources.	The Supplier is compliant this Requirement. The Supplier shall provide the capability to offload files, media, images and other agreed objects from compute resources.
APPS/R/HOST/013	The Supplier shall provide resilient data centre infrastructure with no single point of failure.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/014	The Supplier shall ensure the replication of data and VMs to the secondary site to provide business continuity in the event of a catastrophic failure at the primary site.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/HOST/015	It shall be possible for the Customer to present their own connections and offer a secure remote access solution that allows assured VPN access to the elevated OFFICIAL domain.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/HOST/016	When the Services (or part thereof) is no longer required a backup of Customer Data shall be provided on request in a mutually agreed extract format. Where appropriate, this shall include an image of the virtual machine.	The Supplier is compliant with this Requirement.
APPS/R/HOST/017	NOT USED	NOT USED
APPS/R/HOST/018	The Supplier shall provide Protected Internet connectivity for the Customer by a direct internet connection from the Supplier's data centres.	The Supplier is compliant with this Requirement.
APPS/R/HOST/019	Subject to the provisions of Call Off Schedule 9 (Software and Assets) relating to support and/or upgrade constraints, the Supplier Solution shall support disparate technologies of varying age (and in some instances, technologies that no longer have vendor support) as such technologies and ages are identified in Call Off Schedule 9 (Software and Assets).	The Supplier is compliant with this Requirement.
APPS/R/HOST/020	The Supplier shall host some case materials (particularly in relation to large cases) outside of the CMS.	The Supplier is compliant with this Requirement.
APPS/R/HOST/021	The Supplier shall host Federated Active Directory services as needed to connect with Office 365 services hosted on the Azure platform.	The Supplier is compliant with this Requirement.

1.2 Backup and Recovery

Reference ID	Requirement	Supplier Response
APPS/R/BREC/001	The Supplier shall safeguard Software and Customer Data against loss or damage. In particular, the Supplier shall: a. take copies of all new and changed Software and Customer Data on at least a daily basis and restore the most recent versions in the event of a failure; b. maintain full copies of all Software and Customer Data regularly and restore the most recent versions where necessary; c. maintain a log of all backups to enable speedy access and restoration; d. provide all appropriate protection including up-to-date virus protection; and e. restore Customer Data and User-specific Applications upon request from a User, e.g. where a User has inadvertently deleted or corrupted Customer Data.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/BREC/002	In the event of the loss of a Business Critical System, the Supplier shall ensure that Software and Customer Data are fully restored to the state at the point of failure within the relevant Service Levels.	The Supplier is compliant with this Requirement. See response to APPS/R/BREC/001.
APPS/R/BREC/003	The Supplier shall monitor and verify all backups. This will ensure that, in the event of system failure all Non Business Critical System data can be restored from these backups.	The Supplier is compliant with this Requirement. See response to APPS/R/BREC/001.

Reference ID	Requirement	Supplier Response
	Backup of any data held away from the file servers (i.e. on a User Device) will be the responsibility of the User.	The backup of EUDs is the responsibility of the Customer.
APPS/R/BREC/004	The Supplier shall provide resilient data centre infrastructure with no single point of failure.	The Supplier is compliant with this Requirement. See response to APPS/R/HOST/013.
APPS/R/BREC/005	On request by the Customer, the Supplier shall restore the most recent version of Customer Data to a point not exceeding one (1) Working Day previously.	The Supplier is compliant with this Requirement. See response to APPS/R/BREC/001.
APPS/R/BREC/006	The Supplier shall provide redundant disk architecture for Business Critical Systems such that the loss or failure of a part of the architecture does not cause loss of data for that Service i.e. the data is stored in multiple locations. In addition, the Supplier shall perform a daily backup of Customer Data held on Business Critical Systems	The Supplier is compliant with this Requirement. See response to APPS/R/BREC/001.
APPS/R/BREC/007	The Supplier Solution shall promote data backup to the cloud, as a location-agnostic (UK-based), secure and cost-effective alternative to storing backups on unreliable tape media or expensive local disk solutions.	The Supplier is compliant with this Requirement. See response to APPS/R/HOST/014. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/BREC/008	The Supplier shall enable the transfer of valuable but seldom used Customer Data to a cost efficient, reliable and secure repository, to migrate seldom accessed data to more cost effective storage solution.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further

Reference ID	Requirement	Supplier Response
		information under Section 43(1) of the FOI Act 2000.
APPS/R/BREC/009	The Supplier Solution shall promote archiving to the cloud as a means of storing valuable but seldom used data to a cost-effective, reliable and secure cloud storage repository via PSN, the internet and other networks.	The Supplier is compliant with this Requirement. See response to APPS/R/HOST/014 and APPS/R/BREC/007.

2. Application Support

1. CMS, WMS, MIS

Reference ID	Requirement	Supplier Response
APPS/R/GFUNC/001	The Supplier shall allow the Customer to add or remove Business Critical Systems using the Change Control Procedures.	The Supplier is compliant with this Requirement. The Supplier shall allow the Customer to add or remove Business Critical Systems using the Change Control Procedures.
APPS/R/GFUNC/002	The Supplier will be responsible for seeing all data centre infrastructure, Business Critical Systems, Non Business Critical Systems, and other infrastructure service related incidents through to resolution.	The Supplier is compliant with this Requirement. The Supplier will see all data centre infrastructure, Business Critical Systems, Non Business Critical Systems, and other infrastructure service related incidents in relation to the Services scope through to resolution.

1.1 General Case Facilities (CG)

Reference ID	Requirement	Supplier Response
APPS/R/GCASE/001	The following will apply to the functional specifications in this Section 1 (i.e., 1.1 to 1.49 but excluding Section 1.48), Apps/R/GENNFUN/017 and APPS/R/GENNFUN/019 below: • The Supplier will provide CMS / WMS / MIS functionality in accordance with the Functional Specifications named in the VDR at the time of RFP issue. The Supplier and the Customer shall	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	work together as part of Services governance. If it is demonstrated that the Functional Specifications were inaccurate at the time of RFP issue or updates to CMS / WMS / MIS have been made since RFP issue, any resulting changes to CMS / WMS / MIS shall be subject to the Change Control Procedure.	
APPS/R/GCASE/001A	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CG1 (18.00) CMS FS Cases subsystem • 453001_08_CG2 (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.2 General Case Facilities (WCG)

Reference ID	Requirement	Supplier Response
APPS/R/GCASEW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications:	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	• 453001_08_WCG1 (18.00) WMS FS Case subsystem • 453001_08_WCG2 (18.00) WMS FS Case subsystem	

1.3 Case Allocation (CA)

Reference ID	Requirement	Supplier Response
APPS/R/CASAL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CA (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.4 Case Allocation (WCA)

Reference ID	Requirement	Supplier Response
APPS/R/CASALW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCA (18.00) WMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.5 Structured Bundling (CB)

Reference ID	Requirement	Supplier Response
APPS/R/SBUND/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CB (18.00) CMS FS Cases Bundles	The Supplier is compliant with this Requirement.

1.6 Counts and Indictments Preparation (CC)

Reference ID	Requirement	Supplier Response
APPS/R/COUN/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CC (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.7 Case Pre-Charge Decision (CD)

Reference ID	Requirement	Supplier Response
APPS/R/PCHARG/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CD (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.8 Case Progression Functionality (CE)

Reference ID	Requirement	Supplier Response
APPS/R/CASEPRG/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CE (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.9 WMS Case Progression Functionality (WCE)

Reference ID	Requirement	Supplier Response
APPS/R/CASEPRGW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCE (18.00) WMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.10 Confiscation Cases (CF)

Reference ID	Requirement	Supplier Response
APPS/R/CONFC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CF (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.11 Output Production (CO)

Reference ID	Requirement	Supplier Response
APPS/R/OPROD/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CO (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.12 Output Production (WCO)

Reference ID	Requirement	Supplier Response
APPS/R/OPRODW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCO (18.00) WMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.13 Output Generation

Reference ID	Requirement	Supplier Response
APPS/R/OGEN/001	The Supplier shall ensure that the template and the fields contained therein remain unchanged except via the Change Control Procedure once Approved by the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Customer The standard template and fields are set in the functional specifications: • 453001_G (18.00) CMS FS Generated Outputs • 453001_G (18.00) WMS FS Generated Outputs	

1.14 Print View

Reference ID	Requirement	Supplier Response
APPS/R/PRINT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_H (18.00) CMS FS Print Views • 453001_H (18.00) WMS FS Print Views	The Supplier is compliant with this Requirement.

1.15 Hearing Preparation (CP)

Reference ID	Requirement	Supplier Response
APPS/R/HEARP/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications:	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	• 453001_08_CP (18.00) CMS FS Cases subsystem	

1.16 Case Review (CR)

Reference ID	Requirement	Supplier Response
APPS/R/CREV/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CR (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.17 Case Transfer (CT)

Reference ID	Requirement	Supplier Response
APPS/R/CTRAN/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_CT (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.18 Case Transfer (WCT)

Reference ID	Requirement	Supplier Response
APPS/R/CTRANW/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCT (18.00) WMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.19 Victim Code Communications (VC)

Reference ID	Requirement	Supplier Response
APPS/R/VCC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_VC (18.00) CMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.20 WMS Victim Code Functionality (WVC)

Reference ID	Requirement	Supplier Response
APPS/R/WVC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WVC (18.00) WMS FS Cases subsystem	The Supplier is compliant with this Requirement.

1.21 Hearings Subsystem (H) - CMS

Reference ID	Requirement	Supplier Response
APPS/R/HCMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_09 (18.00) CMS FS Hearings Subsystem	The Supplier is compliant with this Requirement.

1.22 Hearings Subsystem (H) - WMS

Reference ID	Requirement	Supplier Response
APPS/R/HWMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_09 (18.00) WMS FS Hearings Subsystem	The Supplier is compliant with this Requirement.

1.23 Materials (M)

Reference ID	Requirement	Supplier Response
APPS/R/MAT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MR (18.00) CMS FS Material	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Subsystem	

1.24 Electronic Receipt of Unstructured Material (MU)

Reference ID	Requirement	Supplier Response
APPS/R/UNSTRUMU/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MU (18.00) CMS FS Material Subsystem	The Supplier is compliant with this Requirement.

1.25 Electronic Receipt of Structured Material (ME)

Reference ID	Requirement	Supplier Response
APPS/R/UNSTRUME/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_ME (18.00) CMS FS Material Subsystem	The Supplier is compliant with this Requirement.

1.26 Electronic Receipt of Structured Material (MP)

Reference ID	Requirement	Supplier Response
APPS/R/STRUMP/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07_MP (18.00) CMS FS Material Subsystem	The Supplier is compliant with this Requirement.

1.27 CMS Material Archiving (MA)

Reference ID	Requirement	Supplier Response
APPS/R/CMSMA/001	The Supplier shall implement archiving functionality for records in line with the Customer Archiving Policy. The following strategy will be implemented for Case Material in the CMS: a. Three months after a case is concluded (finalised or discontinued), the case will be flagged as archived, unless it has already been marked as of long-term interest. At this point, the CMS will set a retention period for the case. The period will depend on the type of the case, as specified in the Records Management Manual in the Bibliography. b. The Case Material for all archived cases will be retained on-line and Users will be able to search for and access Case Material for archived cases by specifying a flag in the search criteria. Users will be able to search for 'live' cases (the default),	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	or 'archived' cases, or both. c. The CMS will monitor the retention periods for all archived cases and when a retention period expires the CMS will provide facilities to destroy the case by removing all data and documents from the system and will write a case destruction record to the ERMS. When a case is marked as of long-term interest, it will be retained in the CMS database and will not be flagged as archived. The CMS will transfer ownership of these cases to the Customers Records Management Unit three months after the conclusion of the case. d. The CMS will provide facilities for Users to forward cases to the Customer Records Management Unit where the allocated lawyer thinks there should be a review before the case is destroyed, or for cases that are subject to a preservation order under section 17(2) of the Criminal Appeal Act 1995. The Customer Records Management Unit Users will use the CMS to manage, review and when appropriate destroy these cases.	
APPS/R/CMSMA/002	For information: the detailed functional specification is set out within the document titled "453001_07_MA (18.00) CMS FS Material Subsystem".	As APPS/R/GCASE/001.

1.28 User Interface Requirements

Reference ID	Requirement	Supplier Response
APPS/R/UIR/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_14 (18.00) CMS FS User Interface Requirements • The Style Guide is set out at 453001_D (18.00) CMS FS User Interface Style Guide	As APPS/R/GCASE/001.

1.29 Control (L)

Reference ID	Requirement	Supplier Response
APPS/R/CONTL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_05 (18.00) CMS FS Control subsystem	As APPS/R/GCASE/001.

1.30 Control (WL)

Reference ID	Requirement	Supplier Response
APPS/R/CONTW/001	The Supplier shall deliver the functionality as set out in	As APPS/R/GCASE/001.

Reference ID	Requirement	Supplier Response
	the detailed functional specifications: • 453001_05 (18.00) WMS FS Control subsystem	

1.31 Monitor (T)

Reference ID	Requirement	Supplier Response
APPS/R/MONT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_06 (18.00) CMS FS Monitor Subsystem	The Supplier is compliant with this Requirement.

1.32 Monitor (WT)

Reference ID	Requirement	Supplier Response
APPS/R/MONWT/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_06 (18.00) WMS FS Monitor Subsystem	The Supplier is compliant with this Requirement.

1.33 Report (R) – CMS

Reference ID	Requirement	Supplier Response
APPS/R/RCMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_10 (18.00) CMS FS Report Subsystem	The Supplier is compliant with this Requirement.
APPS/R/RCMS/002	The Supplier shall ensure that all standard MIS reports can be run, without the Customer having to request any special access to data	The Supplier is compliant with this Requirement.
APPS/R/RCMS/003	The Supplier shall when requested, run ad-hoc SQL reports	The Supplier is compliant with this Requirement.

1.34 Report (WR) – WMS

Reference ID	Requirement	Supplier Response
APPS/R/RWMS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_10 (18.00) WMS FS Report Subsystem	The Supplier is compliant with this Requirement.

1.35 Configuration (F)

Reference ID	Requirement	Supplier Response
APPS/R/CONF/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_11 (18.00) CMS FS Configuration	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Subsystem	

1.36 Configuration (WF)

Reference ID	Requirement	Supplier Response
APPS/R/CONWF/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_11 (18.00) WMS FS Configuration Subsystem	The Supplier is compliant with this Requirement.

1.37 Support (S)

Reference ID	Requirement	Supplier Response
APPS/R/SUPPS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_12 (18.00) CMS FS Support Subsystem	The Supplier is compliant with this Requirement.

1.38 Support (WS)

Reference ID	Requirement	Supplier Response
APPS/R/SUPPWS/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_12 (18.00) WMS FS Support Subsystem	The Supplier is compliant with this Requirement.

1.39 Screen Layout

Reference ID	Requirement	Supplier Response
APPS/R/SCREEN/001	There are a number of screens that make up CMS and its sub systems. The Supplier shall ensure these screens remain unchanged except via change control and once agreed with the Customer. The screen layouts are further detailed in the following documents: a. 453001_B (18.00) CMS FS Configuration Subsystem Screen Layout; b. 453001_B (18.00) CMS FS Control Subsystem Screen Layout; c. 453001_B (18.00) CMS FS Hearings Subsystem Screen Layout;	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response

	d. 453001_B (18.00) CMS FS Material Subsystem Screen Layout;
	e. 453001_B (18.00) CMS FS Report Subsystem Screen Layout;
	f. 453001_B (18.00) CMS FS Support Subsystem Screen Layout;
	g. 453001_B(W) (18.00) WMS FS Case Subsystem Screen Layout;
	h. 453001_B(W) (18.00) WMS FS Control Subsystem Screen Layout;
	i. 453001_B(W) (18.00) WMS FS Hearings Subsystem Screen Layout;
	j. 453001_B(W) (18.00) WMS FS Report Subsystem Screen Layout;
	k. 453001_B(W) (18.00) WMS FS Support Subsystem Screen Layout;
	l. 453001_B (18.00) CMS FS Case Subsystem Screen Layout;
	m. 453001_B(W) (18.00) WMS FS Material Subsystem Screen Layout;
	n. CD121_453001_B(W) (18.00) WMS FS Configuration Subsystem Screen Layout.	

1.40 Logical Data Model

Reference ID	Requirement	Supplier Response
APPS/R/LDM/001	The Supplier shall ensure that the logical data model and all entities and attributes contained therein remain unchanged except via change control and once agreed with the Customer. The logical data model is detailed within the document titled “453001_C (18.00) CMS FS Logical Data Model”	The Supplier is compliant with this Requirement.

1.41 Management Information System (MIS)

Reference ID	Requirement	Supplier Response
APPS/R/MIS/001	The Supplier shall ensure that the MIS described therein remains unchanged except via change control and once agreed with the CUSTOMER. The SUPPLIER shall deliver the functionality as set out in the following documents: • 553001 (13.00) MIS Functional Specification • 553001 (13.00) MIS Functional Specification - Appendices	The Supplier is compliant with this Requirement.

1.42 Reporting

Reference ID	Requirement	Supplier Response

Reference ID	Requirement	Supplier Response
APPS/R/REP/001	The Supplier shall ensure that the reporting described therein remains unchanged except via change control and once agreed with the Customer. The Supplier shall deliver the functionality as set out in: • 553001 (13.00) MIS Functional Specification – Reports	The Supplier is compliant with this Requirement.

1.43 WMS Manual Entry

Reference ID	Requirement	Supplier Response
APPS/R/WMSM/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_07 (18.00) WMS FS Material Subsystem	The Supplier is compliant with this Requirement.

1.44 CMS External Interface requirements

Reference ID	Requirement	Supplier Response
APPS/R/CMSX/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications:	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	• 25501706 (1.00) Police XML Interface Business Process Document	

1.45 Police Interface – Version 2

Reference ID	Requirement	Supplier Response
APPS/R/POL/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 50403021 (1.2) Two-Way Police XML Interface Business Process Document	The Supplier is compliant with this Requirement.

1.46 Courts Interface

Reference ID	Requirement	Supplier Response
APPS/R/COURTI/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: a. <10705711002 CMS to CCDCS ICD 1.00>; and b. "50404010 CMS API Interface Control Document (2.02)"	The Supplier is compliant with this Requirement.

1.47 Interface with Common Platform

Reference ID	Requirement	Supplier Response
APPS/R/INTFC/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 107 05 72 06 04 CMS to C2I DX Functional Design v1 4	The Supplier is compliant with this Requirement.

1.48 CMS Interface requirements - Witness Care Community Portal (WCCP)

Reference ID	Requirement	Supplier Response
APPS/R/INWCCP/001	As and when reasonably required the Supplier shall hold regular meetings with the other CJO's (Government participants in Criminal Justice Integration Unit (CJIU) or its successor), especially the Police and Courts, to present updates to the corporate standard for Information Management and so facilitate the vision of an electronic and joined-up CJS.	The Supplier is compliant with this Requirement.
APPS/R/INWCCP/002	The Supplier shall, where agreed, represent the Customer at the appropriate CJIU committees.	The Supplier is compliant with this Requirement.

1.49 Data Currency

Reference ID	Requirement	Supplier Response
APPS/R/DATCUR/001	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 453001_08_WCA (18.00) WMS FS Cases subsystem	As APPS/R/GCASE/001.

2. Evidence Management System (EMS)

2.1 EMS - Data Management

2.1.1 Case Creation

Reference ID	Requirement	Supplier Response
APPS/R/EMSCC/001	The following will apply to Section 2 below (i.e., 2.1 to 2.3, inclusive): • The Supplier will provide EMS functionality "as is" at the time of RFP issue. The Supplier and the Customer shall work together as part of Services governance to keep the EMS functionality and Documentation under review. Any resulting changes to EMS shall be subject to the Change Control Procedure.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/EMSCC/001A	The Supplier shall ensure that a case management structure is defined within the system. This structure will enable the storage and organisation of Case Material. The structure must be configurable. *Examples of a typical structure are given in the Case Creation business scenario* The exact structure required shall be defined by the Customer business process which is subject to continuous improvement practices.	The Supplier is compliant with this Requirement.
APPS/R/EMSCC/002	The Supplier shall ensure that the system enables the creation of case structure templates which can be applied on a case by case or Operational Unit basis.	The Supplier is compliant with this Requirement.
APPS/R/EMSCC/003	The Supplier shall ensure that a case can be created in the system irrespective of whether there is Case Material available to store under that case (‘an empty case’). *Simply put, cases many be created and left empty until such time that Case Material becomes available.*	The Supplier is compliant with this Requirement.
APPS/R/EMSCC/004	The Supplier shall ensure that a case can be marked as active or closed.	The Supplier is compliant with this Requirement.
APPS/R/EMSCC/005	The Supplier shall ensure that the system provides an interface and an API if necessary, that allows the creation of a new empty case.	The Supplier is compliant with this Requirement.

2.1.2 Data Input

Reference ID	Requirement	Supplier Response
APPS/R/EMSDI/001	The Supplier shall ensure that Case Material can be manually added to the system from any portable media storage device which is mountable on Windows XP, Vista, Windows 7 and Windows 8 operating systems.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/002	The Supplier shall ensure that Case Material can be manually added to the system from any internal network location which is accessible via Customer devices.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/003	The Supplier shall provide for the automatic ingest of Case Material, where the system is able to monitor network locations and upload data to a configured case and destination as appropriate.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/004	The Supplier shall ensure that the system provides industry standard software interfaces through which data can be ingested and exported. *Web Services would carry particular merit.*	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/005	The Supplier shall ensure that Case Material can be added to a case at any stage unless the case is marked as closed.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/006	The Supplier shall ensure that the digital file types defined in the system specification are ingested by the system.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/EMSDI/007	The Supplier shall ensure that at ingest, the source file can be copied to central storage by the system, with the centrally held case file considered the reference.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/008	The Supplier shall ensure that at ingest, the source file can be indexed in its current location, with the source file location considered the reference.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/009	The Supplier shall ensure that all available file metadata is captured at the file ingest stage. *This includes general file metadata such as date and file size, and file metadata specific to the file type (where available) such as image resolution.*	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/010	The Supplier shall ensure that the system enables the capture of additional metadata against an item or group of items at ingest. *Examples include item reference numbers or category identifiers. A specific example from the Central Fraud Group can be found in the Case Creation business scenario.*	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/011	The Supplier shall ensure that Case Material in a machine-readable-document format is indexed at ingest by the system.	The Supplier is compliant with this Requirement.
APPS/R/EMSDI/01	The Supplier shall ensure that Case Material which is in an	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
2	image representation of text format shall have OCR techniques applied at ingest, with the resulting text being indexed. *This refers specifically to documents which have been scanned and had no OCR layer applied.*	

2.2 EMS – Search & Processing

2.2.1 Viewing Case Material

Reference ID	Requirement	Supplier Response
APPS/R/EMSSP/001	The Supplier shall ensure that the system presents a User configurable interface. Specifically, the size of viewing panes and presence or absence of tool bars and widgets etc. is customisable.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/002	The Supplier shall ensure that Case Material metadata can be viewed without viewing the Case Material itself. In general, it should not be arduous to navigate between cases and categories of case material.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/003	The Supplier shall ensure that Microsoft Office, Adobe and Microsoft Windows generated text documents are viewable from within the system User interface, without	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	reliance on native Applications.	
APPS/R/EMSSP/004	The Supplier shall ensure that all document formats are viewable from within the system User interface, without reliance on native Applications.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/005	The Supplier shall ensure that where emails are viewed it is possible to view any attachment associated with the email	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/006	The Supplier shall ensure that image files can be viewed from within the system User interface, without the reliance on native Applications.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/007	The Supplier shall ensure that video replay is achieved from within system User interface, without the reliance on native Applications.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/008	The Supplier shall ensure that audio replay is achieved from within system User interface, without the reliance on native Applications.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/009	The Supplier shall ensure that all Case Material can be downloaded to the User's device, and that Case Material can be replayed, viewed or edited using the native application.	The Supplier is compliant with this Requirement.
APPS/R/EMSSP/0	The Supplier shall ensure that when viewing lists of case material, the material can be sorted according to the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
10	metadata described in APPS/R/EMSDI/009 and APPS/R/EMSDI/010.	
APPS/R/EMSSP/011	The Supplier shall ensure that when viewing lists of case material, the list can be manually reordered into any order required by the User.	The Supplier is compliant with this Requirement.

2.2.2 Search & Retrieve

Reference ID	Requirement	Supplier Response
APPS/R/EMSSR/001	The Supplier shall ensure that all case material is capable of search based on the case nomenclature described in APPS/R/EMSCC/001 and APPS/R/EMSCC/004.	The Supplier is compliant with this Requirement.
APPS/R/EMSSR/002	The Supplier shall ensure that all case material is capable of search based on the metadata descried in APPS/R/EMSDI/009 and APPS/R/EMSDI/010	The Supplier is compliant with this Requirement.
APPS/R/EMSSR/003	The Supplier shall ensure that all case material is capable of search according to keywords and phrases. This should include all indexed text under APPS/R/EMSDI/011 and APPS/R/EMSDI/012. This requirement includes the ability to search the bundles created under APPS/R/EMSEBC/001.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/EMSSR/004	The Supplier shall ensure that all case material is searchable according to the criteria defined in APPS/R/EMSPCM/015 and APPS/R/EMSPCM/016.	The Supplier is compliant with this Requirement.

2.2.3 Processing of Case Material

Reference ID	Requirement	Supplier Response
APPS/R/EMSPCM/001	The Supplier shall ensure that the system enables multiple Users to work on the same case concurrently.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/002	The Supplier shall ensure that case material can be re-categorised from its categorisation at ingest.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/003	The Supplier shall ensure that relationships can be created between files. The minimum capability shall be the creation of 1:1 relationships between items. Examples include email-attachment and statement-exhibit.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/004	The Supplier shall ensure that Microsoft Office, Open Document Format and all other document file types can be converted to PDF using the system.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/005	The Supplier shall ensure that PDF documents can be split into component documents or combined into a	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	single document using the system.	
APPS/R/EMSPCM/006	The Supplier shall ensure that the page order of a PDF document can be edited using the system.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/007	The Supplier shall ensure that configuration management within the system enables the version tracking of case material which is either edited using the system or undergoes a “check out” and “check in” process.	The Supplier is compliant with this Requirement.
The Supplier shall ensure that the system can enable the following User driven capability when items are processed to include:		
APPS/R/EMSPCM/008	The redaction of document and image file content.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/009	The redaction of audio and video file content.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/010	The annotation of a file.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/011	The capture of comments or notes against a file.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/012	The highlighting of elements within a document.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/013	The rotation of an image.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/014	The addition of hyperlinks within a PDF document.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/EMSPCM/015	The Supplier shall ensure that the tracking of a single item of Case Material and the capture of decision making which supports the Customer business process shall be enabled by the system. Examples of this include marking an item as “reviewed”, “used” or “unused”. The complete Customer business process will be provided at a later stage. The Customer business process is governed by a continuous improvement process and as such this element of the system should be configurable to meet changing requirements as they arise.	The Supplier is compliant with this Requirement.
APPS/R/EMSPCM/016	The Supplier shall ensure the capture of rationale to support the decision making described in APPS/R/EMSPCM/015.	The Supplier is compliant with this Requirement.

2.3 EMS - Presentation of Case Material

2.3.1 Evidence Bundle Creation

Reference ID	Requirement	Supplier Response
APPS/R/EMSEBC/001	The Supplier shall ensure that the system enables the creation of an “evidence bundle”, whereby a selection of case material is compiled into a single PDF document. The Supplier shall ensure that this can be achieved either directly by the system or by interfacing to a third party	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	product to perform the bundling using standard or custom bundling parameter specified by the system. The Supplier shall ensure that the bundle content can either be defined manually, or can be complied according to the decisions recorded under APPS/R/EMSPCM/015. The Supplier shall ensure that the order of documents and pages within the bundle can be defined by the User and that documents and pages are capable of being reordered or removed if necessary. The Supplier shall ensure that the bundle will be paginated according to requirements which shall be presented at a later stage and may be complex. The Supplier shall ensure that a bundle index will be auto generated with hyperlinks to the indexed sections. The Supplier shall ensure that hyperlinks can be added between references in the bundle. The Supplier shall ensure that bundles are able to include any item of case material (with the exclusion of video and audio file types), including any redacted (or otherwise edited) or configuration managed version of a case material item. The Supplier shall ensure that an evidence bundle is accessible from within the system. The Supplier shall ensure that an evidence bundle is compatible with both Windows and Apple Mac operating systems.	

Reference ID	Requirement	Supplier Response
	It should be noted that an evidence bundle can constitute hundreds or in some instances thousands of pages. In addition, the Customer's formatting and pagination requirements are bespoke.	

3. SharePoint

Reference ID	Requirement	Supplier Response
APPS/R/SHAREP/001	The Supplier shall provide hosting and support for the Customer's Knowledge and Information Management systems, including SharePoint. Development of the systems may be requested by the Customer via the Change Control Procedure.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

4. Support of servers and data hosted outside the data centres

Reference ID	Requirement	
APPS/R/SERVSUP/001	NOT USED.	NOT USED.

Reference ID	Requirement	
APPS/R/SERVSUP/002	NOT USED.	NOT USED.

5. Active Directory

Reference ID	Requirement	
APPS/R/ACTIVD/001	The Supplier shall maintain AD Active Directory for Users. This shall include hosting and managing the Customer Public Key Infrastructure in support of active directory domains and certification services.	The Supplier is compliant with this Requirement. The Supplier will maintain and manage Active Directory services.
APPS/R/ACTIVD/002	As part of its Active Directory management responsibilities, the Supplier shall host and manage distributed domain controllers within Supplier data centres in support of active directory domains and certification services.	The Supplier is compliant with this Requirement.
APPS/R/ACTIVD/003	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.	The Supplier is compliant with this Requirement. See response to APPS/R/HOST/021.
APPS/R/ACTIVD/004	The CPS claims an exemption from publishing further	The Supplier is compliant with this Requirement.

Reference ID	Requirement	
	information under Section 43(1) of the FOI Act 2000.	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

6. BES

Reference ID	Requirement	Supplier Response
APPS/R/BES/001	**The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.**	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

7. Email services

Reference ID	Requirement	Supplier Response
APPS/R/EMAIL/001	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/EMAIL/002	Email gateways	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

8. Group Policy Objects

Reference ID	Requirement	Supplier Response
APPS/R/GROUPP/001	The Supplier shall allocate User accounts to organisational units (OUs) based upon the Customer office at which Users' personal file data and account information are stored.	The Supplier is compliant with this Requirement
APPS/R/GROUPP/002	The Supplier shall use OU's to host computer accounts for servers, the various EUD types and administrative User accounts.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GROUPP/003	The Supplier shall take over and use the Group Policy Objects (GPOs) on the OUs in order to control the configuration of EUDs and to restrict access to Applications and generally provide a consistent and secure desktop environment.	The Supplier is compliant with this Requirement. The Supplier shall take over and use the Group Policy Objects (GPOs) on the OUs in order to control the configuration of EUDs and to restrict access to Applications and generally provide a consistent and secure desktop environment.

9. Juniper Remote Access

Reference ID	Requirement	Supplier Response
APPS/R/JRA/001	For Remote Access Services (currently a Juniper solution), the Supplier shall provide a secure approved remote access service allowing all Users the ability to connect to central services over the internet utilising both wired and wireless connections.	The Supplier is compliant with this Requirement.

10. Solidus access

Reference ID	Requirement	Supplier Response
APPS/R/SOLI/001	The Supplier shall provide firewalls, terminal services and certificate services in support of the third party Solidus service.	The Supplier is compliant with this Requirement.

11. Two Factor Authentication System ActivCard

Reference ID	Requirement	Supplier Response
APPS/R/2FACT/001	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information

Reference ID	Requirement	Supplier Response
		under Section 43(1) of the FOI Act 2000.

A.3 Business Critical Systems- Non Functional Requirements

1. General

Reference ID	Requirement	Supplier Response
APPS/R/GENNFUN/001	Subject to APPS/R/AVAMAN/003 the Supplier shall make the Systems available for use at all times unless the Systems have to be shut down for planned maintenance or upgrade. In particular the Supplier shall agree communications with the relevant Customer Representative in respect of: (i) notifying Users of any planned withdrawal of service and (ii) providing Users with regular reminders of all planned withdrawals of service.	The Supplier is compliant with this Requirement. The Supplier shall make the Systems available for use at all times unless the Systems have to be shut down for planned maintenance or upgrade subject to APPS/R/AVAMAN/003.
APPS/R/GENNFUN/002	Subject to APPS/R/AVAMAN/003, the Supplier shall keep outages agreed to withdraw Services, to a minimum. All outages shall be agreed via operational change, and shall be confined to the outage window as agreed by the Change Advisory Board.	The Supplier is compliant with this Requirement. The Supplier shall keep outages agreed to withdraw Services, to a minimum. All outages shall be agreed via operational change, and shall be confined to the outage window as agreed by the Change Advisory Board. A joint CAB will be held regularly between the Supplier and the Customer. This is a forum to discuss, query and authorise upcoming and ongoing changes, and to review past Change. The Supplier recognises the demands of the Customer's business, and will arrange outages at the

Reference ID	Requirement	Supplier Response
		most suitable time as agreed with the CAB and subject to APPS/R/AVAMAN/003.
APPS/R/GENNFUN/003	The Supplier shall ensure that the Services continue to be of sufficient capacity to meet the Customer's operational needs. This includes providing sufficient capacity to cater for growth in use over the Call Off Contract Period.	The Supplier is compliant with this Requirement.
APPS/R/GENNFUN/004	The Supplier shall enable the Customer to respond to urgent requirements for change in the CJS by providing a fast-track mechanism for amending and enhancing the functionality of the CMS. Such mechanism to be agreed during Implementation.	The Supplier is compliant with this Requirement. There is a process for managing urgent changes in Call Off Schedule14 (Change Control Procedures). The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GENNFUN/005	The Supplier shall provide database backup and operating system updates	The Supplier is compliant with this Requirement. See response to APPS/R/BREC/001. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GENNFUN/006	The Supplier shall where possible, use remote management techniques to ensure that fixes to problems can be applied without needing engineers to physically attend site.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further

Reference ID	Requirement	Supplier Response
		information under Section 43(1) of the FOI Act 2000.
APPS/R/GENNFUN/007	The Supplier shall provide the flexibility to "fast track" certain changes, where urgent requirements for change have been identified by the Customer. Call Off Schedule 14 (Change Control Procedure) articulates the process for handling such Change.	The Supplier is compliant with this Requirement.
APPS/R/GENNFUN/008	The Supplier shall ensure that, where possible without detriment to the effective and efficient prosecution of cases, COTS products provided in support of case management are suitable for wider application across the Customer.	The Supplier is compliant with this Requirement. The Supplier will, where possible, utilise COTS products that are suitable for wider application across the Customer.
APPS/R/GENNFUN/009	The Supplier shall make all information exchange agreements and interface specifications freely available for use by Related Suppliers and organisations without charge. The Customer shall be responsible for putting in place any confidentiality arrangements in place with such Related Suppliers and organisations, as needed.	In the case of external interface specifications and agreed information exchange agreements produced by the Supplier, the Supplier shall make such documentation freely available for use by Related Suppliers and organisations without charge.
APPS/R/GENNFUN/009A	Subject to APPS/R/AVAMAN/003, the Supplier shall design the Business Critical Systems solution to be highly resilient to make the Services available to the Customer 24 hours a day, 7 days a week	The Supplier is compliant with this Requirement. The Supplier shall design the Business Critical Systems solution to be highly resilient to make the Services available to the Customer 24 hours a day, 7 days a week.
APPS/R/GENNFUN/010	The Supplier shall allow access to the CMS and WMS to non-Customer users on the authority of the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Customer.	
APPS/R/GENNFUN/011	The Supplier shall ensure that it is possible to control access to case files held on the Case Management System and to fields within a case file to a specific User or group of Users.	The Supplier is compliant with this Requirement. As APPS/R/GCASE/001.
APPS/R/GENNFUN/012	The Case Management System shall enable an organisational or functional unit of the Customer to choose whether or not to hold electronic case files or only summary details of some or all of its cases.	The Supplier is compliant with this Requirement. As APPS/R/GCASE/001.
APPS/R/GENNFUN/013	The Supplier shall ensure that it is always possible to print all or part of an electronic case file and the summary details of a case as a report.	The Supplier is compliant with this Requirement. As APPS/R/GCASE/001.
APPS/R/GENNFUN/014	The Supplier shall ensure that the Case Management System is capable of accepting, storing, processing and reporting on financial data in both pounds sterling and euros.	The Supplier is compliant with this Requirement. As APPS/R/GCASE/001.
APPS/R/GENNFUN/015	The Supplier shall perform the necessary administration tasks in support of the Case Management System to ensure that the CMS continues to function efficiently. This shall include database administration activities, backup and archiving activities, restore, system management	The Supplier is compliant with this Requirement. The Supplier shall perform the necessary administration tasks in support of the Case Management System to ensure that the CMS continues to function efficiently. This

Reference ID	Requirement	Supplier Response
	and network management activities such as general monitoring and health checking.	shall include database administration activities, backup and archiving activities, restore, system management and network management activities such as general monitoring and health checking.
APPS/R/GENNFUN/016	The Supplier shall ensure the CMS continues to be developed in a modular fashion, to allow changes and enhancements to only impact one or more modules, thus making it easier and less costly to modify the functionality.	The Supplier is compliant with this Requirement. The Supplier will ensure that CMS continues to be developed in a modular fashion, to allow changes and enhancements to only impact one or more modules, thus making it easier and less costly to modify the functionality.
APPS/R/GENNFUN/017	For CMS and WMS, the Supplier shall provide and maintain screen options to allow Users to choose to produce correspondence in Welsh and print forms in Welsh or bilingual format. For CMS and WMS, the Supplier shall provide the facilities to enable the Customer to develop and maintain document templates in Welsh and bilingual formats to support this functionality. The Supplier acknowledges that the Services shall be delivered in a manner which is compliant with the Welsh Language Act 1993 and with the Welsh language scheme that the Customer is liable to comply with and where required any change required to ensure such compliance shall be subject to the Change Control Procedure. The Supplier shall ensure that it is familiar with the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Customer's current Welsh language scheme which is available at https://www.cps.gov.uk/cymraeg/assets/uploads/files/CYNLLUN%20IAITH%20GYMRAEG%20-%20WELSH%20LANGUAGE%20SCHEME.pdf.	
APPS/R/GENNFUN/018	In consultation with the Customer, the Supplier shall provide a method statement (no more than one page A4) describing how they could deliver the Service under this Call Off Contract to ensure that Users are treated equally whether they require the service in Welsh or English. This method statement shall briefly address: • each key aspect of the service and the anticipated level of Welsh language requirement for this Call Off Contract; • how they will monitor and promote the ability of Users to receive an equal Welsh or English service, and indicate how they would respond to any resulting change in demand for the service to be provided through the medium of Welsh/English.	The Supplier is compliant with this Requirement.
APPS/R/GENNFUN/019	The Supplier shall deliver the functionality as set out in the detailed functional specifications: "453001_15 (18.00) CMS FS Non-functional Requirements"	The Supplier is compliant with this Requirement.

2. EMS Non Functional Requirements

2.1EMS – Administrative

2.1.1 User Management

Reference ID	Requirement	Supplier Response
	The following will apply to Section 2.1 below: • The Supplier will provide EMS non-functionality "as is" at the time of RFP issue. The Supplier and the Customer shall work together as part of Services governance to keep the EMS non-functionality and Documentation under review. Any resulting changes to EMS shall be subject to the Change Control Procedure.	
APPS/R/EMSUM/001	The Supplier shall ensure that User roles can be defined in the system to which User accounts can be assigned.	The Supplier is compliant with this Requirement.
APPS/R/EMSUM/002	The Supplier shall ensure that the permissions and Designated Access Rights can be configured on a per role basis. *This Requirement implies the creation of a tiered User account structure, similar to that described in the roles within the EMS business scenario.*	The Supplier is compliant with this Requirement.

2.1.2 Access Control

Reference ID	Requirement	Supplier Response
APPS/R/EMSAC/001	The Supplier shall ensure that User authentication is performed against Microsoft Active Directory	The Supplier is compliant with this Requirement.
APPS/R/EMSAC/002	The Supplier shall ensure that Designate Access Rights to all data and Case Material in the system can be specified and applied to User roles or specific Users, and that .The level of access control granularity is sufficient to define access rights at case and item level.	The Supplier is compliant with this Requirement.

2.1.3 Management Information

Reference ID	Requirement	Supplier Response
APPS/R/EMSMI/001	The Supplier shall ensure that the system provides sufficient administrative information to enable the management of system resources. *In particular, this requirement refers to storage management, User numbers and system hardware utilisation*	The Supplier is compliant with this Requirement.

2.1.4 Audit

Reference ID	Requirement	Supplier Response
APPS/R/EMSAUD/001	NOT USED.	The Supplier is compliant with this Requirement.
APPS/R/EMSAUD/002	The Supplier shall ensure that the system maintains a record of any User interaction with Case Material where that interaction results in a change to the item or its associated metadata.	The Supplier is compliant with this Requirement.
APPS/R/EMSAUD/003	The Supplier shall ensure that the system maintains a record of all User management activities described in 2.1.1 User Management above.	The Supplier is compliant with this Requirement.
APPS/R/EMSAUD/004	The Supplier shall ensure that the system provides audit data to comply with, or facilitate compliance with, the applicable requirements of the baseline control set found in CESG Good Practice Guide 13. This accounting data shall be exported automatically by a standard method such as syslog	The Supplier is compliant with this Requirement.
APPS/R/EMSAUD/005	The Supplier shall ensure that the system provides audit data to comply with, or facilitate compliance with, the wider requirements of CESG Good Practice Guide 13. In particular the systems shall deliver applicable recordable events and accounting items specified in GPG13 by a standard method such as syslog.	The Supplier is compliant with this Requirement.

B.1 Non Business Critical Systems of High Importance – Functional Requirements

1. Boundary Firewalls

Reference ID	Requirement	Supplier Response
APPS/R/BFIRE/001	The Supplier shall host and support firewalls used on the boundaries of the external interfaces (internet, PSN and Solidus) and internally to maintain the boundary of the Customer and CMS domains and any internal management infrastructure.	The Supplier is compliant with this Requirement.

2. Checkpoint media server

Reference ID	Requirement	Supplier Response
APPS/R/MEDSERV/001	The Supplier shall host and maintain a Checkpoint media server used for providing removable media encryption on selected EUDs	The Supplier is compliant with this Requirement. A Checkpoint media server will be used to provide removable media encryption on selected End User Devices (EUDs).

3. DNS & DHCP

Reference ID	Requirement	Supplier Response

Reference ID	Requirement	Supplier Response
APPS/R/DNSDHCP/001	DNS, DHCP Management (integrated with AD) The Supplier shall host and maintain internal DNS and external DNS forwarding services and provide DHCP services in accordance with defined IP addressing schema agreed with the Customer	The Supplier is compliant with this Requirement.

4. EPO Server

Reference ID	Requirement	Supplier Response
APPS/R/EPOSERV/001	The Supplier shall host and maintain ePO servers. The Supplier shall maintain on the ePO servers an agreed rule set for the HIPS firewall for EUDs. The Supplier shall maintain up to date AV signatures for EUDs on the ePO servers.	The Supplier is compliant with this Requirement. The Supplier shall use an alternative technical solution for maintaining up to date AV signatures for servers.

5. iChange

Reference ID	Requirement	Supplier Response
APPS/R/ICHANGE/001	The Supplier shall host, maintain and administer the commercial change management workflow system.	The Supplier is compliant with this Requirement.

6. Interface to iTrent, Zanzibar, HR & e-Learning, CIS, FARMS and ePayFact

Reference ID	Requirement	Supplier Response
APPS/R/OTHINT/001	The Supplier shall provide the web connectivity for a range of third party bureau services on the PSN and internet. These shall include, but not be limited to, (interfaces / services related to Basware P2P, iPayview, iTrent, Zanzibar, FARMS, ePayFact, Prosecution Application, College e-Learning portal & Civil Service Learning e-Learning portal, etc.)	The Supplier is compliant with this Requirement.
APPS/R/OTHINT/002	NOT USED.	NOT USED.

7. MBAM Server

Reference ID	Requirement	Supplier Response
APPS/R/MBAM/001	The Supplier shall host and maintain the central MBAM server used for the management of BitLocker on EUDs.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

8. Print Queue Management

Reference ID	Requirement	Supplier Response
APPS/R/PRINTQ/001	The Supplier shall host and provide connection to print queues.	The Supplier is compliant with this Requirement.

9. Remote Multi Functional Device Management

Reference ID	Requirement	Supplier Response
APPS/R/MFDEV/001	The Supplier shall host and maintain the environment for Other Supplier's Print services and provide onward routing into the Customer domain.	The Supplier is compliant with this Requirement.

10. SCCM

Reference ID	Requirement	Supplier Response
APPS/R/SCCM/001	The Supplier shall host and maintain centralised SCCM servers and distribute SCCM packages to servers and EUDs, as requested by the Agency Manager. The Supplier shall complete manual installs of low volume apps on-request in accordance with Call Off Schedule14 (Change Control Procedure). The Supplier shall carry out non-SCCM based application installations on EUDs in accordance with Call Off	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Schedule14 (Change Control Procedure).	
APPS/R/SCCM/002	On instruction from the Agency Manager, the Supplier shall update EUD builds via SCCM including the distribution of up to date security patches.	The Supplier is compliant with this Requirement.
APPS/R/SCCM/003	The Supplier shall create SCCM packages for application distributions to both servers and EUDs. For the avoidance of doubt, the Agency Manager will pass to the Supplier the materials required to create packages for deployment to EUDs and the Agency Manager will test the resulting packages prior to distribution by the Supplier.	The Supplier is compliant with this Requirement.
APPS/R/SCCM/004	The Supplier shall maintain server builds including the distribution of up to date security patches	The Supplier is compliant with this Requirement. The Supplier shall maintain server builds including the distribution of up to date security patches.
APPS/R/SCCM/005	The Supplier shall maintain terminal server builds including the distribution of up to date security patches	The Supplier is compliant with this Requirement. The Supplier shall maintain terminal server builds including the distribution of up to date security patches.
APPS/R/SCCM/006	NOT USED.	NOT USED.

11. Server Operating systems (Windows & Unix)

Reference ID	Requirement	Supplier Response
APPS/R/SOS/001	The Supplier shall maintain and security patch all server OSs (Unix and Windows Server). The Supplier shall deploy patches to EUDs via SCCM, on request from the Agency Manager.	The Supplier is compliant with this Requirement.

12. SQL

Reference ID	Requirement	Supplier Response
APPS/R/SQL/001	The Supplier shall host and maintain SQL server instances used in support of miscellaneous Customer applications.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SQL/002	The Supplier shall backup and restore services for the SQL systems used in support of miscellaneous Customer applications.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

13. Terminal Server

Reference ID	Requirement	Supplier Response
APPS/R/TSERV/001	The Supplier shall provide, maintain and support Terminal services infrastructure / services in the data centres.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

14. Unified Threat Management (UTM)

Reference ID	Requirement	Supplier Response
APPS/R/UTM/001	The Supplier shall provide UTM capability for the core firewalls incorporating IDS capabilities.	The Supplier is compliant with this Requirement. See Annex 1 of this Call Off Schedule, A.12.6 and 13.1.

15. Web Filtering

Reference ID	Requirement	Supplier Response
APPS/R/WEBF/001	The Supplier shall provide web filtering including web proxy and white listing services for internet bound traffic	The Supplier is compliant with this Requirement.

B.2 Non Business Critical Systems of High Importance – Non Functional Requirements

1. General

Reference ID	Requirement	Supplier Response
APPS/R/GNFUN/001	The Supplier shall enable access to all of the Customer's applications or application components hosted at the Supplier's data centres.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GNFUN/002	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall provide second and third line support, including database backup and operating system updates for the Customer System and applications.	The Supplier is compliant with this Requirement. The Supplier shall provide second and third line support, including database backup and operating system updates for the Customer's Non Business Critical Systems of High Importance as defined in Section A, B1.
APPS/R/GNFUN/003	The Supplier shall provide a scalable system, so that any growth in Customer capacity requirements can be met, either by increase in server numbers, server processing capability, or data link bandwidth. Any legacy items that cannot be put into the Supplier's Cloud solution for technical reasons will be reviewed on a case by case basis.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GNFUN/004	The Supplier shall ensure server management, including utilities that will enable remote management and monitoring of each server.	The Supplier is compliant with this requirement.

Reference ID	Requirement	Supplier Response
APPS/R/GNFUN/005	The Supplier shall record, maintain and monitor all installed software and, except for Transferring In Software, associated licence details. For Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements	The Supplier is compliant with the Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

C.1 Non Business Critical Systems of Medium Importance – Functional Requirements

1. Support for office moves

Reference ID	Requirement	Supplier Response
APPS/R/SUPMOV/001	The Supplier shall support office moves. The effort for supporting an office move shall be agreed between the Parties under Call Off Schedule14 (Change Control Procedure).	The Supplier is compliant with the Requirement.

2. Apple xServe Server

Reference ID	Requirement	Supplier Response
APPS/R/APPLE/001	NOT USED.	NOT USED.

3. LAN management within the data centres

Reference ID	Requirement	Supplier Response
APPS/R/LAN/001	The Supplier shall maintain the LAN environment for all the data centre services (i.e. hosted services at non Customer Premises).	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
		The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

4. Traffic Management systems

Reference ID	Requirement	Supplier Response
APPS/R/TRAFF/001	The Supplier will provide, for the Supplier Solution, a suitable bandwidth allowance to the internet. The allowance will be able to burst above this allowance in times of high usage.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/TRAFF/002	The Supplier shall provide as part of capacity management both peak and average utilisation of traffic on the internet and PSN links.	The Supplier is compliant with this Requirement.

5. Monitoring systems for switches, servers, storage and firewalls

Reference ID	Requirement	Supplier Response
APPS/R/MONSYS/001	The Supplier shall provide monitoring and health services (currently ACP, WUG and BMC Patrol) for infrastructure services such as switches, servers, storage subsystems	The Supplier is compliant with this Requirement. The Supplier shall provide monitoring and health services for

Reference ID	Requirement	Supplier Response
	and firewalls.	infrastructure services such as switches, servers, storage subsystems and firewalls.

C.2 Non Business Critical Systems of Medium Importance – Non Functional Requirements

1. General

Reference ID	Requirement	Supplier Response
APPS/R/GENMED/001	The Supplier shall enable access to all of the Customer's applications or application components that are hosted at the Supplier's data centres	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GENMED/002	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall provide second and third line support, including database backup and operating system updates for the Customer's applications.	The Supplier is compliant with this Requirement and shall provide second and third line support, including database backup and operating system updates for the Customer's Non Business Critical Systems of Medium Importance as defined in Section A, C1.

Reference ID	Requirement	Supplier Response
APPS/R/GENMED/003	The Supplier shall also maximise the availability of systems that are not Business Critical Systems	The Supplier is compliant with this Requirement. The Supplier will meet the relevant Service Levels as detailed in Call Off Schedule6.
APPS/R/GENMED/004	The Supplier shall provide the ability for the Customer to increase the hours of availability of the Services, as a permanent or temporary measure. Any such increase will be addressed under Change Control.	The Supplier is compliant with this Requirement. The Supplier shall provide the ability for the Customer to increase the hours of availability of the Services, as a permanent or temporary measure under Change Control.
APPS/R/GENMED/005	The Supplier shall provide a scalable system, so that any growth in Customer capacity requirements can be met, either by increase in server numbers, server processing capability, or data link bandwidth. Any legacy items that cannot be put into the Supplier's Cloud solution for technical reasons will be reviewed on a case by case basis.	The Supplier is compliant with this Requirement.
APPS/R/GENMED/006	The Supplier shall ensure server management, including utilities that will enable remote management and monitoring of each server.	The Supplier is compliant with this Requirement.
APPS/R/GENMED/007	The Supplier shall record, maintain and monitor all installed software and, except for Transferring In Software, associated licence details. For Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage;	The Supplier is compliant with the Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

Reference ID	Requirement	Supplier Response
	and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.	

D General Operational/ Technical Requirements

1. Supportability

Reference ID	Requirement	Supplier Response
APPS/R/SUPP/001	Unless otherwise stated in Call Off Schedule 9 (Software and Assets) in respect of items supplied by the Customer, the Supplier shall ensure that support and maintenance of the hardware and software shall, where reasonably possible, be co-terminus with the Call Off Contract.	The Supplier is compliant with this Requirement.
APPS/R/SUPP/002	The Supplier Solution shall demonstrate corporate social responsibility by lowering the carbon cost when compared to the current infrastructure for the equivalent capacity.	The Supplier is compliant with this Requirement. The Supplier shall demonstrate corporate social responsibility by lowering the carbon cost when compared to the current infrastructure for the equivalent capacity.

Reference ID	Requirement	Supplier Response
APPS/R/SUPP/003	The Supplier's supply chain shall demonstrate the use of 'Green IT' throughout the duration of the Call Off Contract.	The Supplier is compliant with this Requirement. The Supplier shall demonstrate the use of 'Green IT' throughout the duration of the Contract Off Contract.
APPS/R/SUPP/004	The Supplier Solution shall, where practicable, use CE marked components from reputable manufacturers that conform to the appropriate Standards and Regulations specified.	The Supplier is compliant with this Requirement.
APPS/R/SUPP/005	The Supplier shall ensure that all components of the hardware and networks shall operate in accordance with their technical specifications.	The Supplier is compliant with this Requirement.

2. Service Performance Reporting

Reference ID	Requirement	Supplier Response
APPS/R/SPR/001	The Supplier shall provide regular and comprehensive Service Performance Monitoring Reports on achievements and trends against Service Levels and on Incidents and issues arising during the previous Service Period. These reports shall provide sufficient information presented in a structured format to enable easy reconciliation with the Supplier's invoices and shall include, at a minimum, monthly figures (against Service Levels) and trends for:	The Supplier is compliant with this Requirement. The Supplier will provide Service Performance Monitoring Reports within its Service Reporting Pack (SRP). Service level achievements will be recorded in the Service Delivery Report (SDR). The CPS claims an exemption from publishing further information

Reference ID	Requirement	Supplier Response
	a. Service availability and performance, including hosting platform availability; b. Incident management including details of Incidents Resolved; outstanding Incidents and the steps being taken to effect permanent solutions and fix times for the different Severity Levels of Incidents; c. Processor utilization; d. Alerts during reporting period; e. Capacity and usage reports (monthly and trend analysis); f. where possible, component availability; g. Business Critical Systems Database file growth; The design of the reports, based on the content identified above, shall be agreed by the Parties during Implementation. The Customer shall retain the right to vary the design and content of such reports thereafter and, if there is any impact to the monthly reporting cycle, the Parties shall discuss and agree any adjustments, as applicable. The Customer reserves the right to challenge the information received and the Supplier shall respond to those challenges in a timely manner as directed by the policies, processes and procedures or otherwise.	under Section 43(1) of the FOI Act 2000.

Reference ID	Requirement	Supplier Response
APPS/R/SPR/002	The Supplier shall produce a Monthly Service Performance Monitoring Report which shall be delivered within 5 Working Days of the Month's end.	The Supplier is compliant with this Requirement.
APPS/R/SPR/003	The Supplier shall produce a Monthly Finance Report which shall be delivered within 8 Working Days of the Month's end.	The Supplier is compliant with this Requirement.

3. License Management

Reference ID	Requirement	Supplier Response
APPS/R/LICMAN/001	The Supplier shall maintain a clearly defined Software policy to ensure that when new or additional software purchases are made by the Supplier, checks are made on: • the availability of un-utilised software that has already been purchased; and • the existence of corporate licence or other such agreements or facilities; and • the need for all Software in use to be legitimately licensed. For Software supplied by the Customer: • the Supplier shall record, maintain and	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.	
APPS/R/LICMAN/002	For Software provided by the Supplier, the Supplier shall use a software licencing tool to monitor the number and type of Licenses in use for all such Software utilised to implement the Supplier Solution to deliver the Services ensuring: b. all Software in use is legitimately licensed. The Supplier will notify the Customer of any unlicensed software that is identified and shall delete any such software, when instructed to do so by the Customer. The Supplier shall not be responsible for replacing unlicensed software; c. all Transferring In Software, Supplier Procured Software and Supplier Exclusive Software in use has been Approved/authorised by the Customer**.** For Transferring in Software: • the Supplier shall record, maintain and monitor operational details relating to usage;	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements. For all Transferring In Software, the Supplier shall ensure optimum use is made of all software, both current and legacy, for which licences are held.	

4. Software Asset Management

Reference ID	Requirement	Supplier Response
APPS/R/SOFTMAN/001	The Supplier shall record all software on the Supplier's CMDB unless otherwise agreed.	The Supplier is compliant with this Requirement.
APPS/R/SOFTMAN/002	As software changes, through either reorganisation, technology refreshment, or because equipment has failed and a replacement has been installed, the Supplier shall record the changes, thus the asset database will be up to date at all times (save to	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	the extent that asset locations have been changed by the Customer without notification to the Supplier).	
APPS/R/SOFTMAN/003	The Supplier shall record, maintain and monitor all installed software and associated licence details.	See APPS/R/LICMAN/002.
APPS/R/SOFTMAN/004	The Supplier shall provide regular software asset reporting to the Customer. The format and frequency of these reports to be agreed during Implementation.	The Supplier is compliant with this Requirement. The format and frequency of these reports shall be agreed during Implementation and will be set out in the SOM, which shall be amended from time to time in consultation with the Customer.
APPS/R/SOFTMAN/005	NOT USED.	NOT USED.

5. Application Decommissioning

Reference ID	Requirement	Supplier Response
APPS/R/APPDEC/001	The Supplier shall develop an Application Decommissioning methodology with input from the Related Suppliers, the Agency Manager and the Customer, for the managed removal of an Application from the Customer ICT Environment,	The Supplier is compliant with this Requirement. The Supplier shall develop and maintain high level policy / process documentation which shall be detailed in the Supplier's SOM.

Reference ID	Requirement	Supplier Response
	including all dependent Interfaces, scripts and Application data.	
APPS/R/APPDEC/002	The Supplier shall maintain and update the Application Decommissioning methodology at least annually, providing it to the Customer for review and Approval.	The Supplier is compliant with this Requirement. The Supplier shall maintain and update the Application Decommissioning Methodology at least annually, providing it to the Customer for review and Approval.
APPS/R/APPDEC/003	The Supplier shall comply with the Approved Application Decommissioning methodology.	The Supplier is compliant with this Requirement. The Supplier shall comply with the Approved Application Decommissioning Methodology.
APPS/R/APPDEC/004	The Supplier shall ensure that all data records relevant to the Application (including the Service Catalogue) are updated within ten (10) Working Days of completion of the decommissioning Process.	The Supplier is compliant with this Requirement.

6. Release & Deployment management

Reference ID	Requirement	Supplier Response
APPS/R/RELDEP/001	The Supplier shall produce an Apps and Hosting Release Schedule and associated Release Plan(s) and issue these to the Agency Manager and the Customer. The Release Schedule will provide details for at least a three month rolling period.	The Supplier is compliant with this Requirement. The Supplier shall produce an Apps and Hosting Release Schedule and associated Release Plan(s) and issue these to the Agency Manager and the Customer. The Apps and Hosting Release Schedule will provide details for at least a three month rolling period.
APPS/R/RELDEP/002	The Supplier shall maintain a record of all software and firmware upgrade and patch updates, updating the records to show when manufacturers issue new versions, which will be reviewed on a regular basis. The Supplier shall make this available to Agency Manager and the Customer on demand.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/RELDEP/003	Except as provided otherwise in Call Off Schedule 9 (Software and Assets) the Supplier shall maintain software and firmware versions of all services provided by them as a minimum to vendor recommendation and will action new versions within 4 weeks of being made available or as agreed with the Customer.	The Supplier is compliant with this Requirement. See response to APPS/R/RELDEP/002.

7. Service Validation and testing

Reference ID	Requirement	Supplier Response
APPS/R/SERVVAL/001	The Supplier shall specify in detail how Releases will be tested and quality-assured.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SERVVAL/002	The Supplier shall submit a release and testing plan for each Release and submit them to an initial assessment by the Agency Manager. The Supplier shall ensure that each Release shall meet stringent Quality Criteria (to be defined and agreed with the Agency Manager).	The Supplier is compliant with this Requirement.
APPS/R/SERVVAL/003	The Supplier shall conduct release testing and test all release components and all tools and mechanisms required for deployment, migration and back out. The Supplier shall via this process ensure that only components which meet stringent Quality Criteria are deployed into the live production environment.	The Supplier is compliant with this Requirement.
APPS/R/SERVVAL/004	The Supplier shall verify with the Agency Manager that conditions (to be defined and agreed with the Agency Manager) are met for the new service to be activated, and to obtain Approval from the Customer that the new service fulfils the agreed Service Level Requirements. In the event that serious Defects are discovered, the actions that should be discharged by each Party shall be decided between the Supplier,	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Agency manager and Customer.	

8. Customer Satisfaction

Reference ID	Requirement	Supplier Response
APPS/R/CUSSAT/001	The Supplier shall adhere to and operate in accordance with Complaint Management Policies, Processes and Procedures as directed by the Customer (These will be made available to the Supplier during Implementation). The Supplier shall have agreed procedures for recording and responding to customer complaints and shall ensure that all complaints are reported in Service Management Reports to the Customer.	The Supplier is compliant with this Requirement.
APPS/R/CUSSAT/002	The Supplier shall assist and co-operate with the Agency Manager in defining and conducting regular Customer satisfaction surveys of the Services they provide and shall have procedures, agreed with the Agency Manager, for responding to any negative output from these surveys.	The Supplier is compliant with this Requirement and shall assist and co-operate with the Agency Manager in defining and conducting regular Customer satisfaction surveys for the Services they provide as detailed in the SOM.

9. Application Development

Reference ID	Requirement	Supplier Response
APPS/R/APPDEV/001	The Supplier Solution shall provide wide support for developer languages and frameworks, where used and= required to support CMS/WMS and the Prosecutor App, .including Net framework, ASP.NET, VB.Net, C#.Net, Javascript, JQuery, Ajax, XAML, Visual Basic 6.0, Visual Studio, Team Foundation Server. In addition to support the Adobe Enterprise Suite (LiveCycle) application Adobe Workbench, Java and Eclipse or similar.	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/002	Where Users are unable to make changes to aspects of the system then the Change Control Procedures shall be used to request such changes to be made by the Supplier. The Supplier shall assess, agree and test each request before rolling it out to Users	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/003	The Supplier shall implement a consistent User interface across all new systems that the Supplier provides. This shall be based around the interface provided by, where applicable, Microsoft Windows and the COTS products employed. The Supplier shall use standard features for all elements of the User interface.	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/004	As part of the design of systems the Supplier provides, the Supplier shall assess the suitability of COTS products for providing the required functionality. Where the product is suitable, the Supplier shall use a COTS product.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	.	
APPS/R/APPDEV/005	Where Customer requirements are such that use of COTS products are not the most cost-effective solution, the Supplier shall provide a bespoke solution, or shall tailor the COTS products to provide the required solution, or shall propose changes to business processes. Similarly, the Supplier shall use portable and scalable technologies to allow systems to be used from different environments e.g. using desktop PCs, laptops.	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/006	The Supplier shall design its systems so that once data has been entered by a User, or where it has been received electronically from another source, that data shall be validated and once this has been done it will not need to be entered again. The data shall be stored in a central database and shall be accessed and shared between applications/screens.	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/007	NOT USED	NOT USED
APPS/R/APPDEV/008	The Supplier shall ensure the distribution of data and software updates and patches will be as per vendor recommendations and implemented with 4 weeks of being made available, unless otherwise agreed with the Customer.	The Supplier is compliant with this Requirement.
APPS/R/APPDEV/009	The Supplier shall maintain a change management capability to ensure that new services and associated	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	training or other adjustments are efficiently integrated into Service Delivery when ready.	

10. Testing

Reference ID	Requirement	Supplier Response
APPS/R/TEST/001	The Supplier shall conduct testing in line with processes that adhere to Call Off Schedule 5 (Testing).	The Supplier is compliant with this Requirement.
APPS/R/TEST/002	The Supplier shall observe a testing strategy that is based upon a series of testing 'phases', each linked to a particular stage in the project life-cycle. For each testing phase, the Supplier shall create various test scripts, based upon the how the system should work, including as defined in the Functional Specification.	The Supplier is compliant with this Requirement.
APPS/R/TEST/003	The Supplier shall conduct, but not be limited to, the following testing life-cycle to establish the integrity of the system tested: a. Module (or Unit) testing– individual 'modules' of software are thoroughly tested for functional and technical correctness; b. Integration testing – modules which have	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	successfully undergone module testing, are tested with each other in order to demonstrate that they integrate correctly; c. System testing – a complete system or product is fully tested for functional and technical correctness against its specifications; d. Services testing as defined in Call Off Schedule 5 (Testing). e. The Supplier shall develop test scenarios to use during the integration, system and acceptance testing phases and will seek guidance from the Customer to ensure that the scenarios are realistic.	
APPS/R/TEST/004	By a combination of methodical design, and rigorous testing based upon this design, the Supplier shall validate all data entered into the system, whether directly or as an import, before it is committed.	The Supplier is compliant with this Requirement.
APPS/R/TEST/005	The Supplier shall use a combination of methodical design and rigorous testing to prove that the system acts according to how it should act including as specified in the Functional Specification. This shall include tests to show that where data transfers require authorisation, such authorisation is requested and received before transmission takes place.	The Supplier is compliant with this Requirement. See APPS/R/TEST/002.
APPS/R/TEST/006	NOT USED.	NOT USED.

Reference ID	Requirement	Supplier Response
APPS/R/TEST/007	All testing shall be conducted using the path to Live Test Environment, and shall not be conducted within the production environment	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/TEST/008	All testing is to be signed off by the Customer via the operational change management process ahead of moving the components tested to the production environment.	The Supplier is compliant with this Requirement.

11. ITA Requirements

Reference ID	Requirement	Supplier Response
APPS/R/ITAREQ/001	The Supplier will provide consultancy to the Customer and analytical assessments themselves or shall recommend the engagement of reputable Sub-Contractors or 3rd parties The Supplier shall ensure a robust testing plan of all ITA related solutions is undertaken prior to the provision being made available to the User to reduce the likelihood of post Implementation issues.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/ITAREQ/002	The Supplier will provide a dedicated single point of contact to work with the Customer to seek out and implement ITA solutions within agreed timescales (usually no more than 50 days from the date of the Customer raising a request or Order) and to agree an approach to undertake user testing to mitigate post Implementation issues of the provision.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/003	The Supplier will work with the Customer to agree an approach for more complex ITA requirements including continuous improvement and investigation for ITA users.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/004	When providing the Service Catalogue, the Supplier shall include ITA products and services to enable prompt delivery of recurring ITA requests.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/ITAREQ/005	The Supplier will provide a service for new ITA requests and those inflight or previously implemented where User needs identify further requirements or fixes. This includes incident investigation and resolution relating to previously delivered ITA Software and hardware.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/006	The Supplier will identify solutions to meet ITA requests, including the procurement, planning and delivery of solutions and reporting on compatibility issues of provision and Customer ITA solutions and	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	provide options to meet the user and business needs of delivering the provision.	
APPS/R/ITAREQ/007	The Supplier will build, install and test solutions to ensure compatibility where Customer hardware and software is upgraded, replaced, developed or implemented.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/008	The Supplier will provide associated training for ITA solutions to enable Users to fully utilise their solutions, at agreed times with the Users and will provide associated training materials for all provision specifically for ITA users to the Customer.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/009	The Supplier shall ensure new developments are utilised to improve the User experience, including but not limited to upgrades to Dragon and JAWS software.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/010	The Supplier will conduct quarterly end of life reviews on ITA related products supplied by the Supplier, and provide the results of such reviews including an impact assessment for the User, and where applicable, schedule User testing of any upgrades.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/011	The Supplier will build, install and test solutions to meet ITA user and business needs as part of the provision or as a separate stream only if agreed by the Customer.	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
APPS/R/ITAREQ/012	The Supplier will provide documentation of all ITA User needs, solutions, end of life services or support, and lessons learned.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/013	The Customer is entitled to require the Supplier to provide solutions for new or existing key ITA Users out of Working Hours.	The Supplier is compliant with this Requirement.
APPS/R/ITAREQ/014	The Supplier will attend monthly reviews of the ITA service with the Customer to review the performance of the service including activity delivered or in flight; lessons learned; risks and issues outstanding; financial spend; minutes; action trackers and agree to act on any corresponding actions.	The Supplier is compliant with this Requirement.

E. Security Requirements

1. General Security

Reference ID	Requirement	Supplier Response
APPS/R/GENSEC/001	The Supplier shall provide the Customer access to Supplier Personnel and Supplier premises as required for the purposes of improving and auditing security.	The Supplier is compliant with this Requirement. See also Annex 1, A.9.1.
APPS/R/GENSEC/002	The Supplier shall provide that its firewalls provide the ability to undertake security event audit logging.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/GENSEC/003	The Supplier shall ensure that named User accounts used by the Supplier's support personnel for server support shall have specific roles/privileges. Generic unnamed administrative accounts will not be allowed unless explicitly authorised by the Customer's Accreditor.	The Supplier is compliant with this Requirement. See also Annex 1, A.9.2.
APPS/R/GENSEC/004	The Supplier shall ensure that the equipment used to provide the Supplier's inter-site links shall be sufficiently secure from tampering and shall alert the operations bridge to a sufficient degree of attempted	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further

Reference ID	Requirement	Supplier Response
	tampering on the basis that the information carried is protectively marked no higher than OFFICIAL-SENSITIVE.	information under Section 43(1) of the FOI Act 2000.
APPS/R/GENSEC/005	The Supplier Solution shall be designed so that it conforms to the security and audit requirements defined in Call Off Schedule 8 (Security).	The Supplier is compliant with this Requirement.
APPS/R/GENSEC/006	Physical measures shall be taken by introducing additional firewalls onto the Customer WAN to prevent unauthorised access to the Customer network from external threat;	The Supplier is compliant with this Requirement. See Annex 1, A.13.1.
APPS/R/GENSEC/007	ATI (advanced threat investigation) The Customer requires a specialist threat based analytics service to augment the Customer's protective monitoring capability. This needs to draw information from the Customer security systems and provide a combination of expert oversight and automated analytics, to detect and respond to advanced network threats and provide malware analysis capabilities	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/GENSEC/008	The Supplier shall carry out regular IT Health Checks (at a frequency to be agreed during Implementation)	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	and present the outcome of such health checks to the Customer	See also Annex 1, A.12.6.
APPS/R/GENSEC/009	The Supplier shall make available their Security Management Plan as and when required by the Customer and keep it up to date	The Supplier is compliant with this Requirement. The Supplier shall provide a Security Management Plan for the Services it supplies.
APPS/R/GENSEC/010	The Supplier shall demonstrate evidence of Protective Monitoring	The Supplier is compliant with this Requirement. See also Annex 1, A.12.4.
APPS/R/GENSEC/011	The Supplier will demonstrate, through a Customer authorised third party, that the infrastructure has been penetration tested, ensuring security and reliability.	The Supplier is compliant with this Requirement. See also Annex 1, A.14.2.

2. Physical Security

Reference ID	Requirement	Supplier Response
APPS/R/PHYSSEC/001	The Supplier shall operate policies and procedures for the hosting environment that support the operation of a safe and secure working environment in offices, rooms, facilities, and secure areas storing / processing Customer Data.	The Supplier is compliant with this Requirement. See also Annex 1, A.11.1.

Reference ID	Requirement	Supplier Response
APPS/R/PHYSSEC/002	The Supplier shall ensure that all Assets identified in Call Off Schedule 9 (Software and Assets) operated by the Supplier to support the hosting of Customer Data and systems must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of all assets utilized to facilitate the hosting of Customer operations shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/PHYSSEC/003	The Supplier shall deploy a combination of physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance (including CCTV), physical authentication mechanisms, reception desks, and security patrols) to safeguard Customer Data and systems.	The Supplier is compliant with this Requirement. See Annex 1, A.11.1.
APPS/R/PHYSSEC/004	Access to areas containing Customer Data, systems and services shall be controlled and monitored by physical access control mechanisms to ensure that only authorized Supplier Personnel are allowed access.	The Supplier is compliant with this Requirement. See Annex 1, A.11.1.
APPS/R/PHYSSEC/005	The Supplier shall manage access to its wider hosting site, such as service areas and other points where unauthorized personnel may enter the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	premises. These shall be monitored, controlled and isolated from systems hosting Customer Data and services to prevent unauthorized data corruption, compromise, and loss. Authorisation shall be obtained from the Customer prior to relocation or transfer of any element of the hosted solution to offsite / alternative premises.	See Annex 1, A.11.1.
APPS/R/PHYSSEC/006	The Supplier shall provide assurance on the effectiveness of the physical security of its hosting arrangements through external validation against a recognized and relevant security standard. The Supplier shall provide evidence of the successful external validation to the Customer prior to seeking the first Milestone Payment on the Implementation Plan, and at the Customer's reasonable request.	The Supplier is compliant with this Requirement. The Supplier shall ensure that controls are structured in accordance with ISO 27001:2013 and ISO 27002:2013 which covers all security domains.
APPS/R/PHYSSEC/007	The Supplier shall deliver a range of environmental controls aligned to recognized best practice which as a minimum shall include temperature and humidity management, fire identification and suppression, static electricity monitoring and power management and resilience	The Supplier is compliant with this Requirement. See Annex 1, A.11.1.

3. Architecture Security

Reference ID	Requirement	Supplier Response
APPS/R/ARCSEC/001	The Supplier shall ensure that all hosting infrastructure handling, storing and processing the Customer's information undergoes an accreditation / assurance process in accordance with the Customer's Accreditation / Assurance Strategy.	The Supplier is compliant with this Requirement. The Supplier shall ensure that the controls provided are structured in accordance with ISO 27001:2013 and ISO 27002:2013 and cover all security domains.
APPS/R/ARCSEC/002	The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and User access to the minimum possible level) to the design and configuration of the hosting infrastructure that will process or store Customer Data.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/ARCSEC/003	The Supplier shall develop, implement and maintain a security governance framework that coordinates and directs its overall approach to the management of the hosting environment and the information processed (e.g. ISO27001 registration / certification).	The Supplier is compliant with this Requirement. The Supplier will implement management controls to control, measure and manage the Implementation. This will be managed through a clear governance framework in accordance with the provisions of the Security Management Plan.
APPS/R/ARCSEC/004	The Supplier shall develop, implement and maintain 'Processes and Procedures' to ensure the operational security of the hosting environment. Such Processes and Procedures shall be formally documented and reflected in ISMS procedures that would support ISO27001 registration / certification.	The Supplier is compliant with this Requirement. See Annex 1, A.12.1.
APPS/R/ARCSEC/005	The Supplier shall ensure that Supplier Personnel are subject to: (i) adequate personnel security	The Supplier is compliant with this Requirement

Reference ID	Requirement	Supplier Response
	screening; and (ii) adequate security education to ensure that they are able to perform their role.	See Annex 1, A.7.1, A.7.2 and A.7.3.
APPS/R/ARCSEC/006	The Supplier shall design and develop services to identify and mitigate threats to security and any risks that such threats may present to Customer Data.	The Supplier is compliant with this Requirement See Annex 1, A.5.11.
APPS/R/ARCSEC/007	The Supplier shall ensure that its supply chain supports (to the satisfaction of the Customer) all of the security principles that the hosting solution claims to implement.	The Supplier is compliant with this Requirement. See Annex 1, A.15.1.
APPS/R/ARCSEC/008	The Supplier shall ensure that, where applicable, the Customer and/or its Agency Manager is provided with the tools required to take appropriate action on any issues or risks that may arise (such as, access to audit and log information to support incident investigation). The Supplier shall ensure that a forensic readiness capability is consistently provisioned in accordance with the requirements of CESG Good Practice Guide No.18 – Forensic Readiness and that it reflects the sensitivity of Customer Data.	The Supplier is compliant with this Requirement. See Annex 1, A.16.1.
APPS/R/ARCSEC/009	The Supplier shall be responsible for security hardening of the hosting infrastructure. Operating systems shall be hardened to provide only necessary ports, protocols, and services to meet Customer business needs and have in place supporting technical controls such as: antivirus, file	The Supplier is compliant with this Requirement. See Annex 1, A.12.6.

Reference ID	Requirement	Supplier Response
	integrity monitoring, and logging as part of their baseline operating build standard.	
APPS/R/ARCSEC/010	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is embedded within the hosting environment and at its perimeter and interfaces with any other network, service, applications or devices.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.
APPS/R/ARCSEC/011	The Supplier shall provide boundary controls within the hosting infrastructure and identify and confirm the security of all connectivity aspects associated with the Customer hosting environment. Separation and segregation shall be achieved by a combination of physical and technical arrangements that have been Approved by the Customer.	The Supplier is compliant with this Requirement. See Annex 1, A.13.1.
APPS/R/ARCSEC/012	Access to all management functions or administrative consoles for systems hosting Customer Data shall be restricted to authorized personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	The Supplier is compliant with this Requirement. See Annex 1, A.9.2.
APPS/R/ARCSEC/013	The Supplier shall establish a change and configuration control process for the hosting	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	environment to: a. Prevent installation of unauthorised software; b. Update & patch known security vulnerabilities in a timely manner; c. Test all patches and updates prior to deployment; d. Implement work-rounds / other controls where delays in fixing vulnerabilities occur.	See Annex 1, A.12.5.
APPS/R/ARCSEC/014	The Supplier shall: a. Provide the Customer with all Customer Data on demand in an agreed open format; b. Have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade; c. Securely destroy all media that has held Customer Data at the end of life of that media in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor); and d. Securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or	The Supplier is compliant with this Requirement. See Annex 1, A.8.1.

Reference ID	Requirement	Supplier Response
	Sensitive Information (or its successor).	
APPS/R/ARCSEC/015	The Supplier shall make available to the Customer and its designated agents any reasonably requested resources including physical access to Sites, facilities and Key Personnel that support the delivery of the services provided.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/ARCSEC/016	The Supplier shall adhere to and directly support compliance with, all relevant 'Codes of Connection' for services accessed by the Customer from the hosting environment.	The Supplier is compliant with this Requirement. See Annex 1, A.13.2.
APPS/R/ARCSEC/017	The Customer and Supplier shall recognise the need for information to be safeguarded under the UK and EU Data Protection regime (including all relevant aspects of GDPR). To that end, the Supplier shall be able to state to the Customer the physical locations in which data may be hosted from, and to confirm that all relevant legal and regulatory frameworks are complied with.	The Supplier is compliant with this Requirement. See Annex 1, A.18.1.
APPS/R/ARCSEC/018	The Supplier shall be responsible for the scope and delivery of IT Healthchecks / Penetration Testing to the satisfaction of the Customer. The Supplier shall offer necessary assistance should the Customer determine that they require additional / independent IT Healthchecks as frequently as reasonably required by the Customer. All IT Healthchecks / Penetration Testing shall be delivered by a CHECK	The Supplier is compliant with this Requirement. See Annex 1, A.14.2.

Reference ID	Requirement	Supplier Response
	'Green' penetration testing service provider.	
APPS/R/ARCSEC/019	The Supplier shall develop a Business Continuity Plan (BCP) and Disaster Recovery arrangements incorporating risks identified in a risk assessment, including malicious, accidental, technical failure and natural events that could disrupt the Customer's business that is reliant upon the services provided by the hosting environment. The plans shall reflect Customer Recovery Time Objectives (RTOs).	The Supplier is compliant with this Requirement. See Annex 1, A.17.1.

4. Encryption

Reference ID	Requirement	Supplier Response
APPS/R/ENCRYP/001	The Supplier shall provide encryption of data at rest that resides within the hosting environment and that which is stored as 'back up' using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (NCSC and formerly CESG) to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA"). Should the Supplier elect to deploy a 'non assured' product, then this shall be Approved by the Customer.	The Supplier is compliant with this Requirement. See Annex 1, A.10.1.

Reference ID	Requirement	Supplier Response
APPS/R/ENCRYP/002	The Supplier shall ensure that data passed between the hosting environment and any other location of access should be similarly encrypted whilst in transit. In the event that the Supplier determines that the risk which encryption mitigates against is managed by some other means, then this shall be formally recorded. In such circumstances, the Customer will, taking full account of 'residual risk,' determine whether the alternative means of data protection are acceptable. The Supplier Solution shall comply with relevant CESG (now NCSC) cryptographic policy, specifically Cryptographic Mechanisms, Algorithms and Protocols, and apply relevant cryptographic assurance requirements (including operational and physical requirements) for the implementation of cryptographic mechanisms (signing certificates and CRLs), the protection of signing keys, the protection of interactions between service elements and the protection of interactions between Case Allocation services and external elements.	The Supplier is compliant with this Requirement. See Annex 1, A.10.1.

5. Environment Protective Monitoring

Reference ID	Requirement	Supplier Response
APPS/R/ENVIRO/001	The Supplier shall deliver a Protective Monitoring regime that is compliant with the requirements of	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	CESG Good Practice Guide No13 – Protective Monitoring for HMG ICT Systems. The solution shall ensure that threats associated with DDOS, MITM, IP Spoofing, Port Scanning, packet sniffing are covered, along with threats that may be 'internal' such as from any party that may have access to hosting arrangements.	See Annex 1, A.12.4.
APPS/R/ENVIRO/002	The Supplier's Protective Monitoring regime shall provide centralized collection, analysis and correlation of information that is generated by security enforcing technologies such as firewalls, IDS/IPS, AV logs etc that relate to the hosting arrangements provided for the Customer.	The Supplier is compliant with this Requirement. See Annex 1, A.13.1.
APPS/R/ENVIRO/003	The Supplier shall ensure the existence of 'accurate time logs' through as a minimum, the provision of a master time source and synchronisation of all device clocks, time stamping of event records and time stamping of alert messages.	The Supplier is compliant with this Requirement. See Annex 1, A.12.5.
APPS/R/ENVIRO/004	The Supplier shall monitor, record, analyse and report upon business traffic crossing the boundaries of the hosting environment, to ensure that such traffic is authorised and in accordance with security policy. Minimum requirements include: a. Malware detection at the perimeter firewall and internal firewall arrangements; b. Reporting of blocked file import attempts at the	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.

Reference ID	Requirement	Supplier Response
	firewall; c. Reporting of blocked file export attempts at the firewall; d. Reporting of allowed file import at the firewall; e. Reporting of allowed file export at the firewall.	
APPS/R/ENVIRO/005	The Supplier shall monitor, record, analyse and report upon activity at the boundary of the hosting environment with a view to detecting suspicious activity. Minimum requirements include: a. Recording packets dropped by boundary firewalls; b. Deployment of IDS along with an appropriate alerting system; c. Recording of suspected attacks and centralized reporting; d. Recording of changes to firewall (and similar) rule sets with activities of Users involved in making changes logged.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/ENVIRO/006	The Supplier shall detect changes to all device status and configurations that form part of the hosting service provided. Minimum requirements include: a. Reporting of Critical host messages; b. Host malware detection records; c. Recording of changes to anti malware	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.

Reference ID	Requirement	Supplier Response
	signature base; d. Logging and reporting of failed file system access attempts; e. Recording of changes to access rights on system folders/directories; f. Recording of change of status in hosts, attached devices and storage volumes; g. Recording of changes to system (registry) or software configuration; h. Recording of changes to files within system folders.	
APPS/R/ENVIRO/007	The Supplier shall monitor internal boundaries and segregations within the hosting environment to detect suspicious activities. Minimum requirements include: a. Reporting of dropped packets at internal firewalls; b. Deployment of IDS within the hosting environment incorporating virtualized aspects; c. Recording of packets passed by internal firewalls; d. Internal system monitoring events at 'critical' or above; e. Authentication failures; f. System console messages at 'error' status;	See Annex 1, A.12.4.

Reference ID	Requirement	Supplier Response
	g. Changes to firewall rule sets; h. User sessions on devices.	
APPS/R/ENVIRO/008	The Supplier shall monitor any temporary connections to the hosting environment made by remote access, VPN or other transient means of connection. Minimum requirements include the recording of: a. Successful sessions; b. All unsuccessful VPN connections; c. Authentication failures; d. Wireless connections (attempted and successful); e. Changes in VPN configuration; f. Authentication failures; g. Change in status of IDS.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/ENVIRO/009	The Supplier shall monitor User/administrator activity and access to ensure accountability and detect unauthorised activity. Minimum requirements include the recording of: a. User sessions; b. User account status changes;	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.

Reference ID	Requirement	Supplier Response
	c. Changes to privileges; d. Use of database or application administration facilities; e. Running of commands and executables.	
APPS/R/ENVIRO/010	The Supplier shall ensure that Critical classes of events are notified in as close to 'real time' as possible. Minimum requirements include the recording of: a. Alert messages routed to Supplier security console; b. Secondary channel alerting, e.g. SMS messaging. c. The solution shall also allow for the provision of customized performance metrics to be reported to the Customer.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

6. Environment Identity and Access Management

Reference ID	Requirement	Supplier Response
APPS/R/ENVID/001	The Supplier shall operate access control policies and procedures and supporting business processes and technical measures, for ensuring appropriate identification and authentication of personnel involved	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.

Reference ID	Requirement	Supplier Response
	in the administration of the hosting environment.	
APPS/R/ENVID/002	The Supplier shall deliver solution that reduces the number of different access arrangements that Users have in support of the corporate objective of 'Single Sign On' (SSO).	The Supplier is compliant with this Requirement. See Annex 1, A.9.2.
APPS/R/ENVID/003	The Supplier shall define procedures and confirm roles and responsibilities for provisioning and de-provisioning of administrative User accounts following the rule of least privilege, based on defined job function.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/ENVID/004	The Supplier shall provide User account management, delivering the following: e. A centralised process to authorise the creation and deletion of a User account; f. Full visibility (to authorised personnel) in a single place, on who has access to which resource; g. Ability to ensure that proposed new Users do not already have accounts elsewhere; h. Facilitate changes on a 'group' basis rather than at the individual User level.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/ENVID/005	The Supplier shall provide all Users with visibility of the resources they have been granted access to and	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	to those that they may be able to request access to in order to work more effectively.	See Annex 1, A.9.2
APPS/R/ENVID/006	The Supplier shall support simple 'job movement' by allowing Users who change their jobs / roles to be able to retain the same access credentials with updates taking place in the background.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1
APPS/R/ENVID/007	The Supplier shall ensure that 'authentication' is risk based and supported by a centralised policy framework. The policy framework shall allow for the deployment of multifactors for authentication, which can be augmented as a result of the sensitivity and/or risk to the hosting environment at any given time. Any authentication system / product used shall allow for the deployment of 3rd party factors.	The Supplier is compliant with this Requirement. See Annex 1, A.9.2
APPS/R/ENVID/008	The Supplier shall identify, assess, and prioritize risks associated with any third-party access to the hosting environment by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Risk management controls shall be implemented prior to providing access to any third party.	The Supplier is compliant with this Requirement. See Annex 1, A.13.2
APPS/R/ENVID/009	The Supplier shall ensure timely de-provisioning of administrator access to the hosting environment in accordance with established policies in the event of change to a User's status (e.g., termination of employment or other business relationship, job	The Supplier is compliant with this Requirement. See Annex 1, A.9.2.

Reference ID	Requirement	Supplier Response
	change, or transfer).	
APPS/R/ENVID/010	The Supplier shall provide centralized administration of the ID&AM regime for the hosting environment. Centralized administration shall deploy management tools in order to have complete visibility of the ID&AM regime.	The Supplier is compliant with this Requirement. See Annex 1, A.9.2.
APPS/R/ENVID/011	The Contactor shall ensure that administrative Users are managed through a centralised policy driven approach. Privileges shall be allocated and managed using a centralised management facility, which provides visibility and control of systems and services that Users have access to.	The Supplier is compliant with this Requirement. See Annex 1, A.13.2.
APPS/R/ENVID/012	The Contactor shall ensure that 'privileged Users' are managed in the same way as any User, through a centralised policy driven approach. Privileges shall be allocated and managed using a centralised management facility, which provides visibility and control of systems and services that privileged Users have access to.	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/ENVID/013	The Supplier shall implement an ID&AM regime that deploys a centralised function to monitor and report activity including: f. Suspicious login attempts / failed logins;	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.

Reference ID	Requirement	Supplier Response
	g. Monitor access patterns; h. Allowing for tailored and scalable monitoring of User / activities when required; i. Identify unknown / unrecognised access devices and locations; j. Centralised logging and analysis of 'security events'.	
APPS/R/ENVID/014	The Supplier shall ensure that access to, and use of, audit tools that support the operation of the hosting environment's identity and access management regime shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/ENVID/015	The Supplier shall implement an ID&AM regime that maintains security and event related information in a manner that ensures forensic integrity is retained. Arrangements shall support swift intervention following the identification of an incident, which allows for example, immediate suspension of an account across all instance of its use. The Supplier shall be responsible for integration into wider Customer incident response procedures, in order to ensure a consistent response irrespective of incident type.	The Supplier is compliant with this Requirement. See Annex 1, A.16.1.

Reference ID	Requirement	Supplier Response
APPS/R/ENVID/016	The Supplier shall provide a service for Directory Services centralised access requests. Whilst 'automation' is an accepted enabling objective, the Supplier shall ensure that this process does not undermine the requirement for appropriate business authorisation of access requests.	The Supplier is compliant with this Requirement.
APPS/R/ENVID/017	The Supplier shall deliver centralisation of Directory Services providing a single interface to manage all Users, groups and devices that are within the scope of the services provided. This single interface shall deliver integration, deal with requests from applications and directories and support effective password management through application of policy requirements.	The Supplier is compliant with this Requirement.

7. Anti Virus and Malware

Reference ID	Requirement	Supplier Response
APPS/R/ANTVIR/001	The Supplier shall ensure that applications are protected through an holistic anti-virus and malware prevention and detection regime that delivers layered security against this threat. Additionally, the Supplier shall provide controls for protecting applications against Advanced Persistent Threats (APTs).	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.

Reference ID	Requirement	Supplier Response
APPS/R/ANTVIR/002	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is applied both within the application environment and at its perimeter and interfaces with any other network, service, application or device.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.
APPS/R/ANTVIR/003	The Supplier shall employ automated tools to continuously monitor all services that are provisioned within the application environment for virus and all forms of malware. All malware detection events shall be centrally collated, managed and logged.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/ANTVIR/004	The anti-virus and malware prevention and detection regime shall deploy modern AV/Malware protection that provides assurance on its capability to detect, remove and protect against all 'known' types of Malicious Software.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.
APPS/R/ANTVIR/005	The Supplier shall maintain the anti-virus and malware prevention and detection regime so that it is updated in accordance with extant threat levels. Updates to software supporting the regime shall take place on both a scheduled and threat informed basis.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.
APPS/R/ANTVIR/006	The Supplier shall ensure that updates to the malware prevention and detection regime are pushed out to all services that are provisioned within the scope of this Call Off Contract in a consistent and timely manner.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.

Reference ID	Requirement	Supplier Response
APPS/R/ANTVIR/007	The Supplier shall ensure that its process to download and distribute updates to the anti-virus malware prevention and detection regime does not introduce threats to the application environment. The Supplier shall ensure that all updates are verified and are free from malicious content prior to introduction to the application environment.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.
APPS/R/ANTVIR/008	The Supplier's malware prevention and detection regime shall be integrated with the Customer's wider incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.	The Supplier is compliant with this Requirement. See Annex 1, A.12.2.

8. Vulnerability Management

Reference ID	Requirement	Supplier Response
APPS/R/VUNMAN/001	The Supplier shall deliver a Vulnerability Management regime that provides assurance to the Customer that all potential new threats, vulnerabilities or exploitation techniques, which could affect the hosting environment are assessed and corrective action is taken.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4, A.12.6 and A.16.1

Reference ID	Requirement	Supplier Response
APPS/R/VUNMAN/002	The Supplier shall monitor relevant sources of information relating to threat, vulnerability and exploitation techniques, in order to support the provision of an appropriately informed Vulnerability Management regime.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4, A.12.6 and A.16.1
APPS/R/VUNMAN/003	The Supplier shall consider the severity of threats taking full account of the criticality of Customer Data and services that are hosted in the prioritization of mitigation implementation.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/004	The Supplier shall track all identified vulnerabilities and monitor them until required mitigations have been deployed. Timescales for implementing mitigations to vulnerabilities found within the hosting environment shall be communicated to the Customer.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/005	The Supplier shall act immediately to put mitigations in place for any vulnerability where evidence suggests that it is being exploited 'in the wild'. If there is no evidence that the vulnerability is being actively exploited, and where there is no vendor recommendation then the following timescales shall be considered minimum good practice: *'Critical' patches deployed within 14 calendar days of a patch becoming available*	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.

Reference ID	Requirement	Supplier Response
APPS/R/VUNMAN/006	The Supplier shall provide 'real time' vulnerability scanning and remediation deploying best-in-class Vulnerability Management solutions that deliver comprehensive discovery, tailored to the modern, constantly evolving threat environment.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/007	The Supplier shall provide a Vulnerability Management regime that includes within its scope all assets that fall within the scope of the hosting service being provisioned.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/008	The Supplier shall deliver a Vulnerability Management regime that supports automatic and tailored adjustment of the analysis process, which takes account of changes to the Customer's risk, threat and vulnerability profile.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/009	The Supplier shall undertake appropriate Root Cause analysis of identified vulnerabilities, in order to learn from the mitigation process, to limit the possibility of recurrence. This shall contribute to a pro-active approach to Vulnerability Management that is not limited to simply responding to events.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/010	The Supplier shall provide a Vulnerability Management regime in accordance with these requirements that is consistent for all elements of the hosting service provided	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.

Reference ID	Requirement	Supplier Response
APPS/R/VUNMAN/011	The Supplier shall provide the Customer with a monthly summary report on the 'threat landscape'. This report shall include an analysis of metrics that provides the Customer with an understanding of the threats the Supplier has managed and is facing and should not simply be a summary of statistical information. The Supplier shall undertake intelligent analysis in order to provide the Customer with meaningful information to help determine the assurance profile.	The Supplier is compliant with this Requirement. See Annex 1, A.12.6 and A.16.1.
APPS/R/VUNMAN/012	The Supplier's Vulnerability Management regime shall be integrated with the Customer's wider incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.	The Supplier is compliant with this Requirement. See Annex 1, A.16.1.
APPS/R/VUNMAN/013	The Supplier shall be responsible for the arrangement, delivery and associated costs of all external vulnerability testing (penetration testing / IT Healthchecks) that are required to support the accreditation/assurance requirements of the hosting environment, as determined by the Customer. All independent testing undertaken shall be delivered by an approved organization, normally CHECK. Any independent testing that is not carried out by a CHECK approved company, shall be explicitly authorized by the Customer	The Supplier is compliant with this Requirement. See Annex 1, A12.6, A.14.2 and A.18.2

9. Remote Access Security

Reference ID	Requirement	Supplier Response
APPS/R/RAS/001	The Supplier shall provide remote access services that are consistent with guidance provided in the document, CESG Architectural Patterns – Walled Gardens for Remote Access.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.
APPS/R/RAS/002	The Supplier shall provide assured data-in-transit protection. This shall include the deployment of an IPsec client that is assured to 'Foundation Grade' under CESG's Commercial Product Assurance (CPA) scheme. This assurance shall be against the CESG's IPsec VPN for Remote Working – Software Client (SC) Security Characteristic, configured in accordance with PSN end-state IPsec profile or PSN interim IPsec profile.	The Supplier is compliant with this Requirement. See Annex 1, A.10.1.
APPS/R/RAS/003	The Supplier shall define an 'Access Layer' within a DMZ arrangement, where clients are authenticated and termination of the cryptographic link takes place. A firewall shall be deployed to ensure that only approved VPN traffic can reach the 'gateway'. The 'Access Layer' shall provide protection against network bound attacks such as DDoS.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.
APPS/R/RAS/004	If required, the Supplier shall define a 'Presentation Layer' for an agreed subset of web-based application services to the remote access device. The 'Presentation Layer' shall reside within a DMZ. For such agreed subset, remote access devices shall connect to proxying arrangements and not directly to core application services.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2. The CPS claims an exemption from publishing further

Reference ID	Requirement	Supplier Response
	.	information under Section 43(1) of the FOI Act 2000.
APPS/R/RAS/005	The Supplier shall provide assured data-at-rest protection. Any data stored on remote access devices shall be encrypted with an encryption product that is assured to 'Foundation Grade' under CESG's Commercial Product Assurance (CPA) scheme. This shall be deployed when the device is in its 'rest' state. For 'always on' devices, this encryption shall be deployed when the device is locked.	The Supplier is compliant with this Requirement. See Annex 1, A.10.1.
APPS/R/RAS/006	The Supplier shall deploy an effective authentication process for all devices and the services they access which should include the following aspects: • User to device, whereby the User shall only be granted access to the device following successful authentication to the device; • User to service, whereby the User shall only be able to access services after successful authentication to the service via their device; • Device to service, whereby devices are only granted access following successful authentication to the application environment.	The Supplier is compliant with this Requirement. See Annex 1, A.9.4.
APPS/R/RAS/007	The Supplier shall deploy 'platform integrity and application sandboxing'. Arrangements shall ensure that the remote access device can continue to operate securely in the event of a compromise of an application or component within the platform. Functionality shall support	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.

Reference ID	Requirement	Supplier Response
	the requirement to restrict the capabilities of applications on the device.	
APPS/R/RAS/008	The Supplier shall deploy 'malicious code detection and prevention' controls for the remote access service. Arrangements shall detect, isolate and defeat malicious code, which may have achieved ingress to the remote access architecture.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.
APPS/R/RAS/009	The Supplier shall ensure effective 'security policy enforcement' to ensure that policies set by the enterprise are implemented in remote access devices. It shall be possible to centrally enforce a set of security policies on devices and ensure that these policies cannot be circumvented by the device User or unauthorised entity.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.
APPS/R/RAS/010	The Supplier shall deploy 'external interface protection' ensuring that remote access devices are limited to an agreed profile, the number of ports (physical and logical) and services exposed to untrusted networks and devices.	The Supplier is compliant with this Requirement. See Annex 1, A.6.2.2.
APPS/R/RAS/011	The Supplier shall deploy 'event collection' for all elements of the remote access service, to report security events to a centrally provisioned audit and monitoring arrangement. This facility shall be restricted from the User and mitigate against unauthorised access attempts.	The Supplier is compliant with this Requirement. See Annex 1, A.12.4.
APPS/R/RAS/012	The Supplier shall deploy an 'incident response'	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	arrangement that integrates with wider response procedures in place across the Customer ICT Environment.	See Annex 1, A.12.4 and A.16.1.

10. Security Architecture and Design

Reference ID	Requirement	Supplier Response
APPS/R/SECARC/001	The Supplier shall ensure that all systems / applications handling, storing and processing the Customer's information undergo an accreditation / assurance process in accordance with the Customer's Accreditation / Assurance Strategy.	The Supplier is compliant with this Requirement. See Annex 1, A.18.2.
APPS/R/SECARC/002	The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and User access to the minimum possible level) to the design and configuration of systems / applications / services which will process or store Customer Data (aka Designated Access Rights).	The Supplier is compliant with this Requirement. See Annex 1, A.9.1.
APPS/R/SECARC/003	The Supplier shall ensure that any transmission of Customer Data is adequately protected against tampering, denial of service, eavesdropping and virus ingress.	The Supplier is compliant with this Requirement. See Annex 1, A.13.2.
APPS/R/SECARC/004	The Supplier shall ensure that Customer Data (and the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	assets storing or processing such Customer Data), shall be adequately protected against physical tampering, loss, theft, damage or seizure.	See Annex 1, A.11.2.
APPS/R/SECARC/005	The Supplier shall ensure that an adequate degree of separation exists between different Users of the services provided by the systems / applications. This should prevent anyone malicious or compromised from affecting the provision of the services or the security of Customer Data.	The Supplier is compliant with this Requirement. See Annex 1, A.6.1.2.
APPS/R/SECARC/006	The Supplier shall develop, implement and maintain a security governance framework that coordinates and directs its overall approach to the management of the systems / applications / services and the information processed (e.g. ISO27001 registration / certification).	The Supplier is compliant with this Requirement See Annex 1, A.5.1.1.
APPS/R/SECARC/007	The Supplier shall develop, implement and maintain 'Processes and Procedures' to ensure the operational security of the services provided. Such Processes and Procedures shall be formally documented and reflected in ISMS procedures that would support ISO27001 registration / certification.	The Supplier is compliant with this Requirement See Annex 1, A.12.1.
APPS/R/SECARC/008	The Supplier shall ensure that Supplier Personnel are subject to: (i) adequate personnel security screening; and (ii) adequate security education to ensure that they are able to perform their role.	The Supplier is compliant with this Requirement See Annex 1, A.7.1, A.7.2 and A.7.3.
APPS/R/SECARC/009	The Supplier shall design and develop services to identify	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	and mitigate threats to security and any risks that such threats may present to Customer Data.	• The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SECARC/010	The Supplier shall ensure that its supply chain supports (to the satisfaction of the Customer) all of the security principles that the Supplier Solution claims to implement.	The Supplier is compliant with this Requirement See Annex 1, A.15.1.
APPS/R/SECARC/011	The Supplier shall ensure that, where applicable, the Customer and/or its Agency Manager is provided with the tools required to help the Customer securely manage the services and to take appropriate action on any issues or risks that may arise (such as, access to audit and log information to support incident investigation). The Supplier shall ensure that a forensic readiness capability is consistently provisioned in accordance with the requirements of CESG Good Practice Guide No.18 – Forensic Readiness and that it reflects the sensitivity of Customer Data.	The Supplier is compliant with this Requirement See Annex 1, A.16.1.
APPS/R/SECARC/012	The Supplier shall ensure that access to all Service interfaces is limited to authenticated and authorised Users only.	The Supplier is compliant with this Requirement See Annex 1, A.15.1.
APPS/R/SECARC/013	The Supplier shall ensure that all external or less trusted interfaces of the system / application / service are identified and have appropriate protections to defend against attacks through such interfaces. These protections shall be configured in accordance with	The Supplier is compliant with this Requirement See Annex 1, A.13.1.

Reference ID	Requirement	Supplier Response
	architectural arrangements outlined in CESG Good Practice Guide No.8 – Protecting External Connections to the Internet.	
APPS/R/SECARC/014	The Supplier shall ensure that the methods used by Supplier Personnel to manage the services provided, mitigates any risk of exploitation that could undermine the security of the services and provides full accountability for their activities.	The Supplier is compliant with this Requirement See Annex 1, A.12.1.
APPS/R/SECARC/015	The Supplier shall be responsible for the scope and delivery of IT Healthchecks / Penetration Testing to the satisfaction of the Customer. The Supplier shall offer necessary assistance should the Customer determine that they require additional / independent IT Healthchecks as frequently as reasonably required by the Customer. All IT Healthchecks / Penetration Testing shall be delivered by a CHECK 'Green' penetration testing service provider.	The Supplier is compliant with this Requirement. • The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SECARC/016	The Supplier shall put in place technical policies and controls which include patching (within vendor-recommended timeframes) against known vulnerabilities. The Supplier shall ensure that security vulnerabilities and weaknesses are reported to the Customer.	The Supplier is compliant with this Requirement See Annex 1, A.12.2 and A.12.6.
APPS/R/SECARC/017	The Supplier shall make available to the Customer and its designated agents any reasonably requested resources including reasonable physical access to Sites, facilities and Key Personnel that support the delivery of the services provided.	The Supplier is compliant with this Requirement. See APPS/R/GENSEC/001. The Supplier will control access to Sites used for the delivery of Services under this Call Off Contract and

Reference ID	Requirement	Supplier Response
		will determine the business need for Customer access to these locations.
APPS/R/SECARC/018	The Supplier shall adhere to and directly support compliance with, all relevant 'Codes of Connection' for services accessed by the Customer.	The Supplier is compliant with this Requirement See Annex 1, A.18.2.
APPS/R/SECARC/019	The Customer and Supplier shall recognise the need for information to be safeguarded under the UK and EU Data Protection regime (including all relevant aspects of GDPR). To that end, the Supplier shall be able to state to the Customer the physical locations in which data may be stored, processed and managed from, and to confirm that all relevant legal and regulatory frameworks are complied with.	The Supplier is compliant with this Requirement See Annex 1, A.18.1.
APPS/R/SECARC/020	The Supplier shall agree any change in location of data storage, processing and administration with the Customer in advance where the proposed location is outside the UK. The Supplier shall be aware of legal requirements regarding the location of data outside of the UK.	The Supplier is compliant with this Requirement See Annex 1, A.18.1.
APPS/R/SECARC/021	The Supplier shall: a. Provide the Customer with all Customer Data on demand in an agreed open format; b. Have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade; c. Securely destroy all media that has held Customer Data at the end of life of that media in line with HMG	The Supplier is compliant with this Requirement See Annex 1, A.17.1.

Reference ID	Requirement	Supplier Response
	Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor); and d. Securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor). The Supplier shall establish a configuration control process to: a. Prevent installation of unauthorised software; b. Update & patch known security vulnerabilities in a timely manner; c. Test all patches and updates prior to deployment; d. Implement work-rounds / other controls where delay in fixing vulnerabilities. The Supplier shall develop a Business Continuity Plan (BCP) incorporating risks identified in a risk assessment, including malicious, accidental and natural events that could disrupt the Customer's business. The BCP shall reflect Customer Recovery Time Objectives (RTOs).	

CATEGORY 3: AGENCY MANAGEMENT REQUIREMENTS

1 SERVICE OPERATIONS

1.1 Service Desk

Reference ID	Requirement	Supplier Response
APPS/R/SDESK/001	The Supplier shall adhere to: (i) the Service Desk Policies, Processes and Procedures; and (ii) guidance on interfacing with the Service Desk as provided to the Supplier by the Agency Manager which may be amended via Call Off Schedule 14 (Change Control Procedure).	The Supplier is compliant with this Requirement. The Supplier shall adhere to the Service Desk Policies, Processes and Procedures and will operate in accordance with the Supplier's SOM. The Supplier will work with the Customer's chosen Service Desk Supplier to establish an efficient working relationship and work to put good knowledge sharing in place. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/002	The Supplier shall interface with the Service Desk such that the Supplier is able to access the Service Desk tool, receive incident records logged by the Service Desk, update, amend and pass back incident records to the Service Desk as necessary.	The Supplier is compliant with this Requirement. The Supplier shall access the Service Desk tool, receive incident records logged by the Service Desk, update, amend and pass back incident records to the Service Desk as necessary. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/003	The Supplier shall interface with the Service	The Supplier is compliant with this Requirement. The Supplier

Reference ID	Requirement	Supplier Response
	Desk such that the Supplier is able to access the Service Desk tool, receive Service Catalogue requests logged by the Service Desk, update, amend and pass back request related records to the Service Desk as necessary**.**	shall access the Service Desk tool, receive Service Catalogue requests logged by the Service Desk, update, amend and pass back request related records to the Service Desk as necessary. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/004	The Supplier shall ensure that, where necessary, the interfaces between the Supplier Systems and the Service Desk shall be automated to allow tickets to be raised automatically between the Supplier Systems and the Service Desk tool	The Supplier is compliant with this Requirement. The Supplier shall work with the Agency Manager to automate, where necessary and possible, the interfaces between the Supplier Systems and Service Desk to allow tickets to be raised automatically between the Supplier Systems and the Service Desk tool.
APPS/R/SDESK/005	The Supplier shall provide advice and support to the Customer's staff and Users on the operation of the Supplier Solution.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/006	The Supplier shall provide feedback to Users and /or the Agency Manager on progress made with resolving an Incident. Such feedback shall include: (i) advice on any remedial action being taken; (ii) the estimated date and time when the Incident may be Resolved; (iii) and advice	The Supplier is compliant with this Requirement. The Supplier shall provide feedback to Users on the progress of an Incident in accordance with the Service Desk PPPs and will operate in accordance with the Supplier's SOM.

Reference ID	Requirement	Supplier Response
	allowing the User to continue to use the Services until such time as the Incident is Resolved.	
APPS/R/SDESK/007	NOT USED.	NOT USED.
APPS/R/SDESK/008	The Supplier shall develop Application Support and data hosting PPPs for the delivery of the Services.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/009	The Supplier shall interface with the Service Desk provided by the Agency Manager such that the Supplier is able to receive Incident and requests records logged by the Service Desk, update, amend and pass back Incident records to the Service Desk as necessary.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/010	The Supplier shall contribute to the Knowledge Management System and the Known Error Log provided by the Agency Manager to support improved Incident analysis.	The Supplier is compliant with this Requirement The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SDESK/011	NOT USED	NOT USED
APPS/R/SDESK/012	The Supplier shall ensure that Root Causes to Incidents and problems are addressed, and that Workarounds that continue to exist while the Root Cause is addressed are reported each	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

Reference ID	Requirement	Supplier Response
	Service Reporting Period.	

1.2 Incident Management

Reference ID	Requirement	Supplier Response
APPS/R/INCMAN/001	The Supplier shall investigate and resolve all Incidents in accordance with the Service Levels, including: a. assessing the probable cause of each Incident; b. testing and replacing or repairing faulty hardware/software as required; and c. carrying out any other procedures as required to facilitate the resolution of the Incident.	The Supplier is compliant with this Requirement. The Supplier shall use its extensive knowledge of the Supplier systems to investigate and resolve Incidents in accordance with the Service Levels. Clear links and interactions will be put in place between the various Incident management processes of the Supplier, Customer and Related Suppliers to ensure an effective overall Incident management process.
APPS/R/INCMAN/002	Where an Incident relates to security, the Supplier shall maintain the forensic integrity of systems following an Incident in accordance with good practice defined within 'CESG Good Practice Guide No 18 – Forensic Readiness'.	The Supplier is compliant with this Requirement. The Incident management solution will include an Incident investigation capability, which is 'CESG Good Practice Guide No 18 – Forensic Readiness' compliant.
APPS/R/INCMAN/003	The Supplier shall promptly complete agreed corrective actions as agreed with the Agency Manager.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

Reference ID	Requirement	Supplier Response
APPS/R/INCMAN/004	The Supplier shall promptly notify the Agency Manager of any Incident that is known to have breached or is likely to breach the Service Levels or that has, in the opinion of the Supplier, been incorrectly allocated.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/INCMAN/005	The Supplier shall; (i) update the Incident record with all relevant information to ensure that Root Cause analysis can be carried out by the Agency Manager; and (ii) co-operate with the Agency Manager as required for the Agency Manager to carry out Root Cause analysis.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/INCMAN/006	Where the Agency Manager has altered the assigned Incident Severity Level of an Incident in accordance with Customer instructions and agreed this with the Supplier, the Supplier shall resolve such Incident in accordance with the new Incident Severity Level.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/INCMAN/007	The Supplier shall ensure that, in the event that the investigation of an Incident reveals non-compliance of the Supplier Solution with any Requirement set out in this Call Off Contract, then the Supplier shall rectify such non-compliance at no cost to the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	Customer. Such rectification shall be Approved by the Customer and the Agency Manager, in advance and, where necessary, implemented via the Change Control Procedure.	

1.3 Request Management

Reference ID	Requirement	Supplier Response
APPS/R/REQMAN/001	The Supplier shall contribute to and use the Business Service Catalogue including in accordance with the relevant PPP.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/REQMAN/002	The Supplier shall review Management Information on a monthly basis to identify trends or significant changes or increases in service request volumes, for discussion with the Agency Manager and, where necessary, Related Suppliers, as applicable.	The Supplier is compliant with this Requirement. The Supplier shall review and analyse trends of Service request volumes and types.
APPS/R/REQMAN/003	The Supplier shall identify possible Process improvements and promptly make appropriate recommendations to the Agency Manager in writing.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/REQMAN/004	The Supplier shall immediately bring to the attention	The Supplier is compliant with this Requirement. The

Reference ID	Requirement	Supplier Response
	of the Agency Manager any issues that prevent the Supplier from processing Service Requests.	Supplier shall promptly inform the Agency Manager, in accordance with the agreed PPPs, of any issues preventing the Supplier from processing Service Requests.
APPS/R/REQMAN/005	The Supplier shall ensure that Service Requests received from the Agency Manager are expedited within agreed Service Levels when assigned by the Service Desk	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/REQMAN/006	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Agency Manager in response to Service Requests.	The Supplier is compliant with this Requirement. The Supplier shall provide the Agency Manager with relevant information related to the Service Request in accordance with the agreed PPPs.
APPS/R/REQMAN/007	The Supplier shall: (i) co-operate with the Agency Manager to proactively manage and monitor the status and progress of all Service Requests for the Services ordered via the Business Service Catalogue; and (ii) adhere to the PPP relevant to Service Requests as provided by the Agency Manager.	The Supplier shall comply with this Requirement The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/REQMAN/008	The Supplier shall respond to the Agency Manager or the Customer's enquiries regarding Service Requests with accurate and up-to date information.	The Supplier is compliant with this Requirement. The Supplier shall provide the Agency Manager with accurate and up to date information related to the Service Request.
APPS/R/REQMAN/009	NOT USED	NOT USED

1.4 Problem Management

Reference ID	Requirement	Supplier Response
APPS/R/PROBMAN/001	The Supplier shall adhere to the problem management policies, processes and procedures as set out in the Agency Manager's Problem Management Procedure	The Supplier is compliant with this Requirement. The Supplier shall adhere to the Problem Management PPPs and SOM. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/PROBMAN/002	The Supplier shall participate with the Agency Manager in Incident Reviews and Major Incident Reviews, as necessary	The Supplier shall comply with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/PROBMAN/003	The Supplier shall (i) contribute to Major Incident Reports; and (ii) ensuring that Major Incident Reports provide clear details to the Agency Manager as set out in the Problem Management Procedure.	The Supplier is compliant with this Requirement The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

1.5 Access Management

Reference ID	Requirement	Supplier Response
APPS/R/ACCMAN/001	The Supplier shall provide access to systems as requested by the Users in accordance with: (i) the Policies of the Customer and/or Agency Manager	The Supplier is compliant with this Requirement. The Supplier shall provide User access in accordance with the PPPs agreed with the Customer and/or the Agency

Reference ID	Requirement	Supplier Response
	relating to Access Management and (ii) the Supplier's operational Procedures as agreed with the Agency Manager and the Customer.	Manager, and will operate in accordance with the SOM.
APPS/R/ACCMAN/002	The Supplier shall provide appropriate access (including remote access) to the necessary tools and systems to the Agency Manager, thereby enabling the Agency Manager to comply with its responsibility and obligations under its agreement with the Customer.	The Supplier shall comply with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/ACCMAN/003	The Supplier shall reject any access request that has not been properly approved by Agency Manager in accordance with the Access Management Policy.	The Supplier is compliant with this Requirement. The Supplier shall enable only those User access requests that have been approved by the Agency Manager in accordance with the PPPs.
APPS/R/ACCMAN/004	The Supplier shall inform the Agency Manager and the Customer where it suspects or has reason to believe that inappropriate User access has been requested.	The Supplier is compliant with this Requirement. The Supplier shall inform the Agency Manager and/or the Customer in accordance with the PPPs where it suspects inappropriate User access has been requested.
APPS/R/ACCMAN/005	The Supplier shall assist and co-operate with the Agency Manager by granting appropriate access to Related Suppliers to the Supplier System, as applicable.	The Supplier is compliant with this Requirement. The Supplier shall assist and cooperate with the Agency Manager by granting appropriate access to Related Suppliers to the Supplier Systems where agreed via the Change Control Procedure.

2 SERVICE DESIGN

2.1 Availability Management

Reference ID	Requirement	Supplier Response
APPS/R/AVAMAN/001	The Supplier shall design and document the solution to be highly resilient to make the Services available to the Customer whenever possible, normally 24 hours a day, 7 days a week. It is for this reason that the Supplier shall incorporate a high degree of resilience, including, but not limited to, full mirroring of Critical Business Systems, together with well defined fail-over arrangements, thus ensuring that these systems will remain available.	The Supplier is compliant with this Requirement. See also APPS/R/GENNFUN/001.
APPS/R/AVAMAN/002	The Supplier shall design their services such that the duration of any necessary service withdrawal events will be kept to the absolute minimum.	The Supplier is compliant with this Requirement. See also APPS/R/GENNFUN/002.
APPS/R/AVAMAN/003	The Supplier shall strictly manage all proposed service withdrawals, both during Implementation and after each Operational Service commencement, and adhere with the following requirements as a minimum: a. The Supplier shall manage all operational change in accordance with the Policies, Processes and Procedures as directed by the Customer	The Supplier is compliant with this Requirement. Details of the implementation of withdrawals shall be documented in the SOM.

Reference ID	Requirement	Supplier Response
	b. The Supplier shall not withdraw any service for any reason without formal Approval by the Customer. c. The Supplier shall operate on the principle of conducting all service withdrawals during periods when usage monitoring demonstrates they are least utilised over a 24 hour period. d. The Supplier shall operate with the intention of adhering to pre-defined “windows” of planned maintenance/release opportunities throughout the calendar year, to be agreed prior to Service commencement. e. The Supplier shall produce a forward plan of all planned change activity impacting availability of services on a rolling 3 month basis. f. The Supplier shall notify all Planned Service Outages to the Customer in accordance with SL’s in Call Off Schedule 6 (Service Levels, Service Credits and Performance Monitoring). g. The Supplier shall notify all unplanned service withdrawals, or emergency withdrawals which are necessary in order to resolve Incidents, in accordance with the Policies, Processes and Procedures as directed by the Customer.	

2.2 Capacity Management

Reference ID	Requirement	Supplier Response
APPS/R/CAPMAN/001	The Supplier shall provide any reasonable information requested by the Agency Manager in respect of the Agency Manager overall capacity plan and support the on-going maintenance and development of such overall capacity plan.	The Supplier is compliant with this Requirement.
APPS/R/CAPMAN/002	The Supplier shall monitor, analyse and report to the Agency Manager in relation to capacity volumes and trends and shall, where appropriate, act on any capacity related issues.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CAPMAN/003	The Supplier shall provide all such assistance as reasonably requested by the Agency Manager in establishing future capacity requirements for Supplier Systems, based on the Customer's defined business needs and plans. The Supplier shall make recommendations to the Agency Manager regarding how existing capacity plans for the Services are or may be affected by demand projections, and such recommendations shall include the steps needed to meet demand projections.	The Supplier is compliant with this Requirement.
APPS/R/CAPMAN/004	NOT USED.	NOT USED
APPS/R/CAPMAN/005	The Supplier shall provide standard Service Reports which enable continual monitoring and insight into capacity trends. The Supplier shall review these reports and shall	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	provide a dedicated Customer Support Manager to review capacity management on a monthly basis in liaison with the Supplier's technical resources.	The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CAPMAN/006	The Supplier shall manage, control and predict the performance and capacity of Operational Services. This includes initiating proactive and reactive action to address current and future performance and capacity impact of the Operational Services.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CAPMAN/007	The Supplier shall manage, control and predict the performance, utilization and capacity of IT resources and individual IT components (at a level to be agreed during Implementation).	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

3 SERVICE IMPLEMENTATION

3.1 Change Management

Reference ID	Requirement	Supplier Response
APPS/R/CHAMAN/001	The Supplier shall adhere to the Change Control	The Supplier is compliant with this Requirement. The

Reference ID	Requirement	Supplier Response
	Procedures as set out in Call Off Schedule 14 (Change Control Procedure)	Supplier shall adhere to the Change Control Procedures as set out in Call Off Schedule 14 (Change Control Procedure).
APPS/R/CHAMAN/002	The Supplier shall contribute to the Change material in Call Off Schedule 14 (Change Control Procedure) and issue this to the Agency Manager and the Customer.	The Supplier is compliant with this Requirement. The Supplier shall contribute to the Change material in Call Off Schedule 14 (Change Control Procedure) and issue this to the Agency Manager and the Customer in accordance with PPPs agreed with the Agency Manager.
APPS/R/CHAMAN/003	The Supplier shall produce an Apps and Hosting Release Schedule and associated Release Plan(s) and issue these to the Agency Manager and the Customer. The Release Schedule will provide details for at least a three month rolling period.	The Supplier is compliant with this Requirement. See APPS/R/RELDEP/001.
APPS/R/CHAMAN/004	The Supplier shall ensure that vendor recommended patching is applied to all Assets and Software used to deliver the Services under this Call Off Contract, as directed by Agency Manager.	The Supplier is compliant with this Requirement.
APPS/R/CHAMAN/005	The Supplier shall schedule, coordinate and manage Planned Service Outages in accordance with Policies, Processes and Procedures and as directed by the Customer.	The Supplier is compliant with this Requirement. See APPS/R/GENNFUN/002.
APPS/R/CHAMAN/006	The Supplier shall support and assist the Agency Manager by responding to Impact Assessments	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	and shall provide input where required.	
APPS/R/CHAMAN/007	The Supplier shall monitor, analyse and report to the Agency Manager in respect of Change volumes and trends. The format of such reports shall be agreed during Implementation.	The Supplier is compliant with this Requirement. The Supplier shall agree with the Agency Manager the format and content of reports for the volumes and trends of Changes related to Supplier Services, and then provide these reports to the Agency Manager.
APPS/R/CHAMAN/008	The Supplier shall provide all reasonably requested Management Information to the Agency Manager	The Supplier shall comply with this Requirement..
APPS/R/CHAMAN/009	The Supplier shall raise Change Requests in order to make operational or technical Changes to the Services.	The Supplier is compliant with this Requirement. The Supplier shall raise operational change requests in to make operational changes to Supplier Services, as appropriate.
APPS/R/CHAMAN/010	The Supplier shall: • attend the Change Advisory Board (CAB) (including emergency CABs as necessary); • ensure that any issues related to the Supplier raised at the Change Advisory Board meeting are progressed to the satisfaction of Agency Manager; and • where required by the Agency Manager, provide such support reasonably requested to enable the progression of changes owned by Other Suppliers. The Supplier	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	retains the right to request that Project work relating to Other Supplier change may be the subject of a Change Request.	
APPS/R/CHAMAN/011	The Supplier shall track and monitor all approved Changes and ensures that Change records are updated throughout the lifecycle of each Change in accordance with decisions made at the Change Advisory Board.	The Supplier is compliant with this Requirement. The Supplier shall track and monitor all approved Changes to Services and ensures that Change records are updated throughout the lifecycle of each Change in accordance with decisions made at the Change Advisory Board and as agreed in the PPPs.
APPS/R/CHAMAN/012	The Supplier shall ensure that operational change requests contain information including, but not limited to: (i) Implementation Plans; (ii) Test Success Criteria; (iii) Back Out Plans or Remediation Plans; (iv) Plans for handover to support; (v) User communication plans; and (vi) Configuration Items affected.	The Supplier is compliant with this Requirement. The Supplier shall ensure that operational change requests contain information including, but not limited to, as appropriate to the particular change: (i) Implementation Plans; (ii) Test Success Criteria; (iii) Back Out Plans or Remediation Plans; (iv) Plans for handover to support; (v) User communication plans; and (vi) Configuration Items affected.
APPS/R/CHAMAN/013	Following implementation of an operational change, the Supplier shall ensure that Post Implementation Reviews implemented by Agency Manager are carried out and managed effectively, and that any lessons learned from each Post Implementation	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.

Reference ID	Requirement	Supplier Response
	Review are implemented and fed into the assessment of future Changes.	
APPS/R/CHAMAN/014	The Supplier shall ensure that any operational changes that occur more often than three (3) times each rolling monthly period are processed consistently with the requirements of the Agency Manager.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CHAMAN/015	The Supplier shall ensure that all pre-approved Changes are publicised by the Agency Manager in the Service Catalogue.	The Supplier shall comply with this Requirement. The Supplier shall provide approved Service Catalogue items for inclusion in the Agency Manager's Business Service Catalogue.
APPS/R/CHAMAN/016	The Supplier shall: (i) identify any potential Change Management process improvements; (ii) make appropriate recommendations to the Agency Manager; and (iii) where these are agreed by the Customer, the Supplier shall manage any process improvement activity until completed.	The Supplier shall comply with this Requirement. (i) The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CHAMAN/017	The Supplier shall adhere to the governance required by the Agency Manager and/or the Customer regarding Change Requests, including): (i) the raising and recording of Changes;	The Supplier is compliant with this Requirement.

Reference ID	Requirement	Supplier Response
	(ii) the assessment and evaluation of the Change; (iii) the cost and the benefit of the proposed Change; and (iv) the review and closure of Changes.	
APPS/R/CHAMAN/018	In respect of Change, the Supplier shall ensure that all Assets used in delivering the Services adhere at all times to; (i) any hardware vendor support requirements; and (ii) any requirements of the Agency Manager relating to Incident Management.	The Supplier is compliant with this Requirement.
APPS/R/CHAMAN/019	The Supplier shall: (i) ensure that any compatibility issues between the Customer's Systems immediately prior to the Call Off Commencement Date and new or proposed Supplier Systems are identified as soon as reasonably practicable and in any event prior to the date of Achievement of the relevant Operational Services Commencement Date; and (ii) assist and co-operate with the Agency Manager to determine the treatment of such compatibility issues.	The Supplier is compliant with this Requirement.
APPS/R/CHAMAN/020	NOT USED	NOT USED
APPS/R/CHAMAN/021	NOT USED	NOT USED

Reference ID	Requirement	Supplier Response

3.2 Software Asset and Configuration Management (SACM)

Reference ID	Requirement	
APPS/R/SACM/001	The Supplier shall maintain accurate Asset details, including details of the hardware, operating system and any bespoke or packaged Software in order for the Agency Manager to maintain the CMDB.	The Supplier is compliant with this Requirement. The Supplier shall maintain accurate details for the Assets used in the provision of Supplier Services, including details of the hardware, operating system and any bespoke or packaged Software used in the provision of Supplier Services in order for the Agency Manager to maintain the CMDB. See APPS/R/LICMAN/001.
APPS/R/SACM/002	The Supplier shall where necessary carry out Asset disposal; including the procurement of formal certification that secure and environmentally responsible disposal has been conducted, and shall notify the Agency Manager of such disposals, in order for the Agency Manger to maintain the CMDB.	The Supplier is compliant with this Requirement. The Supplier shall carry out Asset disposal as necessary for the Assets used in the provision of Supplier Services; including the procurement of formal certification that secure and environmentally responsible disposal has been conducted, and shall notify the Agency Manager of such disposals, in order for the Agency Manger to maintain the CMDB.
APPS/R/SACM/003	The Supplier shall agree and provide regular reporting to the Agency Manager and the Customer regarding any relevant licence compliance for all Software provided by	The Supplier is compliant with this Requirement. See APPS/R/LICMAN/001.

Reference ID	Requirement	
	the Supplier used to deliver the Supplier Solution. For all Transferring In Software: • the Supplier shall record, maintain and monitor operational details relating to usage; and • the Customer's Agency Manager will be responsible for the management of commercial, licencing and support arrangements.	
APPS/R/SACM/004	The Supplier shall work with the Agency Manager and the Customer, as reasonably required, to confirm the scope of any Asset Management audits and the investigation and resolution of any discrepancies related to Asset Management. Unless agreed otherwise by the Parties, such Asset Management audits shall occur at least once per year during the Call Off Contract Period, at no additional charge to the Customer.	The Supplier is compliant with this Requirement.
APPS/R/SACM/005	The Supplier shall provide the results of Asset Management audit data to the Agency Manager within the timescales and in the format reasonably required by the Agency Manager.	The Supplier is compliant with this Requirement.
APPS/R/SACM/006	The Supplier shall receive, review and, when instructed by the Agency Manager and/or the Customer implement recommendations for Service Asset and Configuration Management process improvements. If the scale and nature of these improvements requires additional resources, this may be subject to agreement under the	The Supplier is compliant with this Requirement.

Reference ID	Requirement	
	Change Control Procedure. .	
APPS/R/SACM/007	The Supplier shall provide CI (Configuration Item) data to the Agency Manager in a format and frequency appropriate for inclusion in the Agency Manager supplied integrated CMDB.	The Supplier is compliant with this Requirement. The Supplier shall provide CI (Configuration Item) data to the Agency Manager in a format and frequency appropriate for inclusion in the Agency Manager supplied integrated CMDB.
APPS/R/SACM/008	The Supplier shall develop, test and implement changes to asset management system interfaces and Configuration Item data content as agreed with the Agency Manager. If the scale and nature of these changes requires additional resources this may be subject to agreement under the Change Control Procedure.	The Supplier is compliant with this Requirement.
APPS/R/SACM/009	The Supplier shall assist and co-operate with the Agency Manager in determining the reason for each Configuration Item discrepancy, its criticality, and actions required to address it.	The Supplier is compliant with this Requirement. The Supplier shall assist and co-operate with the Agency Manager in determining the reason for each Configuration Item discrepancy, its criticality, and actions required to address it.

3.3 Knowledge Management

Reference ID	Requirement	
APPS/R/KNOWM/001	The Supplier shall contribute to the knowledge management system provided by the Agency Manager for the capture, storage, and presentation of information required to manage the Services.	The Supplier is compliant with this Requirement. The Supplier shall contribute to the knowledge management system provided by the Agency Manager for the capture, storage, and presentation of information required to manage the Services in accordance with the PPPs.
APPS/R/KNOWM/002	The Supplier shall ensure that, where data created by the Supplier is found in the knowledge management system provided by the Agency Manager that is inaccurate, incomplete or lacks integrity, such data is promptly corrected.	The Supplier is compliant with this Requirement.
APPS/R/KNOWM/003	The Supplier shall assist and co-operate with the Agency Manager in ensuring the knowledge management system contains data and information, including: i. methods to resolve Incidents; ii Known Errors; iii. Service Desk scripts; iv. build data; v. self-help articles; and vi. frequently asked questions (FAQs).	The Supplier will is compliant with this Requirement. The Supplier shall assist and co-operate with the Agency Manager in accordance with the PPPs.

3.4 Service Implementation

Reference ID	Requirement	Supplier Response

Reference ID	Requirement	Supplier Response
APPS/R/SERVTRA/001	The Supplier shall ensure that the Implementation phase does not interrupt normal operations and availability unless absolutely necessary and, where necessary, should follow the Change Process Policies, Processes and Procedures as directed by the Customer.	The Supplier is compliant with this Requirement.
APPS/R/SERVTRA/002	The Supplier shall define the data migration approach in the Supplier's Implementation Plan.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/SERVTRA/003	User profiles and associated data shall be migrated in a planned and verifiable manner with no loss of data or data integrity.	The Supplier is compliant with this Requirement. See APPS/R/SERVTRA/002.
APPS/R/SERVTRA/004	The Supplier shall ensure that backups can be recovered from the pre-migrated system to the new system once migration has taken place.	The Supplier is compliant with this Requirement. See APPS/R/SERVTRA/002.
APPS/R/SERVTRA/005	The Supplier shall provide a roll back plan as part of each operational change request raised, to mitigate for any issues during transition to the new hardware and software.	The Supplier is compliant with this Requirement See APPS/R/SERVTRA/002 and APPS/R/CHAMAN/012.
APPS/R/SERVTRA/006	The Supplier shall ensure that there are sufficient dry-runs to validate the Data Migration, Cutover and Rollback procedures. The Supplier shall ensure that the disaster recovery environment is available prior to cutover to the Supplier Solution.	The Supplier is compliant with this Requirement. See APPS/R/SERVTRA/002.

Reference ID	Requirement	Supplier Response
APPS/R/SERVTRA/007	Supplier passwords for all applications and systems supported by the Supplier to be reset (where possible remotely) by the Supplier (i) as required by the Agency Manager; or (ii) provided that, if the Supplier is resetting passwords, it will follow the process set out in the SOM.	The Supplier is compliant with this Requirement.

4. I.T. SERVICE CONTINUITY MANAGEMENT (ITSCM)

Reference ID	Requirement	Supplier Response
APPS/R/ITSCM/001	The Supplier shall make sure that all Supplier Personnel with responsibilities for fighting disasters are aware of their exact duties, and to make sure that all relevant information is readily available when a disaster occurs.	The Supplier is compliant with this Requirement. The Supplier shall ensure that all members of Supplier Personnel with responsibilities for disaster recovery relating to Supplier Services are aware of their exact duties, and that all relevant information is readily available to them when a disaster occurs.
APPS/R/ITSCM/002	The Supplier shall design appropriate and cost-justifiable continuity mechanisms and procedures to meet the Business Continuity Plan and Disaster Recovery Plan as set out in Call Off Schedule 10 (Business Continuity and Disaster Recovery). This includes the design of risk reduction measures and recovery plans.	The Supplier is compliant with this Requirement. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/ITSCM/003	The Supplier shall ensure preventive measures and	The Supplier is compliant with this Requirement. The

Reference ID	Requirement	Supplier Response
	recovery mechanisms for disaster events are subject to regular testing.	Supplier shall ensure preventive measures and recovery mechanisms for disaster events associated with Supplier Services are subject to regular testing as agreed in the PPPs.
APPS/R/ITSCM/004	The Supplier shall create and make available to the Customer detailed instructions on when and how the Supplier will invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first steps to be taken by the Supplier upon learning that a (suspected) disaster has occurred.	The Supplier is compliant with this Requirement. The Supplier shall provide detailed instructions to the Customer on when and how the Supplier will invoke disaster recovery procedures associated with Supplier Services, including the first steps to be taken by the Supplier upon learning that a (suspected) disaster has occurred as agreed in the PPPs.

5. SERVICE DESIGN

5.1 Service Catalogue Management

Reference ID	Requirement	Supplier Response
APPS/R/SCM/001	The Supplier shall contribute to and use the Business Service Catalogue.	The Supplier is compliant with this Requirement. The Supplier shall contribute to Business Service Catalogue which is managed by the Agency Manager, by providing a Service Catalogue.
APPS/R/SCM/002	The Supplier shall provide a Service Catalogue, containing all commodity products to be provided by this Supplier. Service Catalogue pro-forma to be agreed during	The Supplier is compliant with this Requirement. The Supplier shall provide a Service Catalogue, containing all commodity products to be provided by the Supplier for inclusion by the Agency Manager in the Business Service

Reference ID	Requirement	Supplier Response
	Implementation	Catalogue. The Service Catalogue pro-forma shall be as defined in the PPPs.
APPS/R/SCM/003	The Supplier shall review Management Information on a monthly basis to identify trends or significant changes or increases in service request volumes, for discussion with the Agency Manager and, where necessary, Related Suppliers, as applicable.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/002.
APPS/R/SCM/004	The Supplier shall identify possible Process improvements and promptly make appropriate recommendations to the Agency Manager in writing.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/003.
APPS/R/SCM/005	The Supplier shall immediately bring to the attention of the Agency Manager any issues that prevent the Supplier from processing Service Requests.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/004.
APPS/R/SCM/006	The Supplier shall ensure that Service Requests received from the Agency Manager are expedited within agreed Service Levels when assigned by the Service Desk	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/005.
APPS/R/SCM/007	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Agency Manager in response to Service Requests.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/006.
APPS/R/SCM/008	The Supplier shall: (i) co-operate with the Agency Manager to proactively manage and monitor the status and progress of all Service	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/007.

Reference ID	Requirement	Supplier Response
	Requests for the Services ordered via the Business Service Catalogue; and (ii) adhere to the PPP relevant to Service Requests as provided by the Agency Manager.	
APPS/R/SCM/009	The Supplier shall respond to the Agency Manager or the Customer's enquiries regarding Service Requests with accurate and up-to date information.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/008.
APPS/R/SCM/010	The Supplier shall manage end of life Service Catalogue items, such that, at least one month before the end of life Service Catalogue item is discontinued, replacement Service Catalogue items: a) are adequately tested (including User acceptance testing where appropriate); b) are Approved by the Customer; c) have any relevant Call Off Contract Charges agreed between the Supplier and Customer; d) added to the Service Catalogue; and e) any relevant Test Environment(s) is created.	The Supplier is compliant with this Requirement. See APPS/R/REQMAN/009.

5.2 Service Level Management

Reference ID	Requirement	Supplier Response
APPS/R/SLM/001	NOT USED	NOT USED
APPS/R/SLM/002	NOT USED	NOT USED
APPS/R/SLM/003	NOT USED	NOT USED
APPS/R/SLM/004	NOT USED	NOT USED
APPS/R/SLM/005	NOT USED	NOT USED
APPS/R/SLM/006	The Supplier to provide a monthly Performance Monitoring Report, and within this report to compare the agreed and actually Achieved Service Levels, and also include information on the usage of services, ongoing measures for service improvement, and any exceptional events that occurred during the period measured.	The Supplier is compliant with this Requirement. The Supplier shall provide a monthly Performance Monitoring Report which will include a comparison of the agreed and actually Achieved Service Levels, and also include information on the usage of Supplier Services, ongoing measures for service improvement, and any exceptional events that occurred during the period measured.

6. CONTINUAL SERVICE IMPROVEMENT

Reference ID	Requirement	Supplier Response

Reference ID	Requirement	Supplier Response
APPS/R/CSI/001	The Supplier shall review all of the services provided by the Supplier on a regular basis, with a view to improving service quality where necessary, and to identify more economical ways of providing a service where possible.	The Supplier is compliant with this Requirement and shall review all of the services provided by the Supplier on a regular basis, with a view to improving service quality where necessary, and to identify more economical ways of providing a service where possible as defined in the PPPs.
APPS/R/CSI/002	The Supplier shall evaluate processes on a regular basis. Such evaluation to include identifying areas where the targeted process metrics are not reached, holding regular benchmarkings, audits, maturity assessments and reviews.	The Supplier is compliant with this Requirement. The Supplier shall evaluate Supplier processes on a regular basis, including identifying areas where the targeted process metrics are not reached, holding regular benchmarkings, audits, maturity assessments and reviews, as appropriate.
APPS/R/CSI/003	The Supplier shall define specific initiatives aimed at improving services and processes, based on the results of service reviews and process evaluations. The resulting initiatives shall either be internal initiatives pursued by the Supplier on its own behalf, or initiatives which require the Customer's cooperation.	The Supplier is compliant with this Requirement. The Supplier shall define specific initiatives aimed at improving Supplier Services and processes, based on the results of service reviews and process evaluations. The resulting initiatives shall either be internal initiatives pursued by the Supplier on its own behalf, or initiatives which require the Customer's cooperation. The CPS claims an exemption from publishing further information under Section 43(1) of the FOI Act 2000.
APPS/R/CSI/004	The Supplier shall verify if improvement initiatives are proceeding according to plan, and introduce corrective	The Supplier is compliant with this Requirement. The Supplier shall verify if improvement initiatives related to

Reference ID	Requirement	Supplier Response
	measures where necessary.	Supplier Services and processes are proceeding according to plan, and introduce corrective measures where necessary in accordance with the PPPs.

Part B, Annex One – Draft Security Management Plan (SMP)

The CPS claims an exemption from publishing this information under Section 43(1) of the FOI Act 2000.