Attachment 1 – Services Specification

FUTURE CASEWORK TOOLS

FCT Applications, Databases and Infrastructure Management Service (ADIMS)

BUSINESS REQUIREMENTS DOCUMENT

VERSION 0.7

04/01/2023

TABLE OF CONTENTS

This Attachment consists of a Part A and a Part B. Part A contains the Buyer's Service Requirements and Part B contains the Supplier Service Descriptions.

Part A – Buyer's Service Requirements

1. INTRODUCTION

1.1 Part A / Part B Scope

1.1.1. This Part A contains the Buyer's Service Requirements for this applications, development and infrastructure management services ("**ADIMS**") Contract.

1.1.2. The Service Requirements under Part A of this Attachment are made up of Functional Requirements, Non-Functional Requirements, Finance Management, Service Transition, and Implementation and Transition.

1.1.3. Scope of the Services

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

1.1.3.1.1. the services, functions, responsibilities, requirements and deliverables that the Supplier is required to carry out as specified in Part A (Service Requirements) of this Attachment and the relevant Schedules and Attachments of the Contract;

1.1.3.1.2. any incidental services, functions, responsibilities, requirements and deliverables not specified in the 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 1.1.3.1.1 above;

1.1.3.1.3. any services, functions, requirements, responsibilities and/or deliverables agreed pursuant to Schedule 5 (Change Control Procedure); and

1.1.3.1.4. 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 Attachment, Schedule S3 (Security Requirements), Schedule S1 (Implementation) and Attachment 3 (Outline Implementation Plan), and Schedule S6 (Business Continuity and Disaster Recovery).

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

1.1.4. If there is any conflict between the scope of the services, functions, responsibilities, requirements and deliverables under: (i) Paragraphs 1.1.3.1.1 and 1.1.3.1.2 above; and (ii) Paragraph 1.1.3.1.4 above, the provisions of Paragraphs 1.1.3.1.1 and 1.1.3.1.2 above shall apply and prevail**.**

1.1.5. 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 Attachment meets and fulfils all of the Service Requirements in this Part A), as the same may evolve during the Contract Period and as they may be supplemented, enhanced, modified or replaced in accordance with this Contract, but excluding any services, responsibilities or functions that are expressly identified in the Order Form as the Buyer's responsibility or a third party's responsibility.

1.1.6. If there is any conflict between the provisions of Part A of this Attachment and the provisions of Part B of this Attachment, the provisions of Part A of this Attachment shall prevail, except that the Buyer is entitled to accept the provision of any conflicting element of Part B where such conflict is in the favour of, or otherwise beneficial to, the Buyer.

1.1.7. Where Part B of this Attachment does not contain a written Supplier Solution for a Service Requirement(s) in Part A of this Attachment, the Supplier agrees and confirms that it shall meet and fulfil such Service Requirement(s).

1.2 The Crown Prosecution Service

The Crown Prosecution Service (CPS) prosecutes criminal cases that have been investigated by the police and other investigative organisations in England and Wales. The CPS is independent, and we make our decisions independently of the police and government.

The CPS has approximately 7500 highly trained staff whose duty is to make sure the right person is prosecuted for the right offence, and that trials are fair so that offenders are brought to justice whenever possible.

The CPS:

- decides which cases should be prosecuted;
- determines the appropriate charges in more serious or complex cases, and advises the police during the early stages of investigations;
- prepares cases and presents them at court; and
- provides information, assistance and support to victims and prosecution witnesses.

Prosecutors must be fair, objective and independent. When deciding whether to prosecute a criminal case, our lawyers must follow the Code for Crown Prosecutors. This means that to charge someone with a criminal offence, prosecutors must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction, and that prosecuting is in the public interest.

The CPS works closely with the police, courts, the Judiciary and other partners to deliver justice.

1.3 How we are organised and operate

The CPS operates across England and Wales, with 14 regional teams prosecuting cases locally. Each of these 14 CPS Areas is headed by a Chief Crown Prosecutor (CCP) and works closely with local police forces and other criminal justice partners.

CPS Areas deal with a wide range of cases. The majority are less serious cases and are heard in the magistrates' courts, while the most serious cases are heard in the Crown Court. CPS Direct, with prosecutors based across England and Wales, provides charging decisions to police forces and other investigators 24 hours a day, 365 days a year.

In addition, CPS Central Casework Divisions deal with some of the most complex cases we prosecute. They work closely with specialist investigators from a range of organisations, including the National Crime Agency, HM Revenue & Customs and the Independent Police Complaints Commission, as well as police forces across England and Wales.

The specialist divisions, each headed by a Head of Division (equivalent to a Chief Crown Prosecutor), are:

- Serious Economic, Organised Crime and International Directorate (SEOCID), including CPS Proceeds of Crime (CPSPOC)
- Special Crime and Counter Terrorism Division

All operational divisions are supported by our headquarters directorates, which cover the primary support functions for CPS, including Finance and Commercial directorate, Human Resources, Strategy and Policy, Communications, Operations and Digital and Information Directorate.

1.4 Our values

1. We will be independent and fair
2. We will prosecute independently, without bias and will seek; to deliver justice in every case.

3. We will be honest and open
4. We will explain our decisions, set clear standards about the service the public can expect from us and be honest if we make a mistake.
5. We will treat everyone with respect
6. We will respect each other, our colleagues and the public we serve, recognising that there are people behind every case.
7. We will behave professionally and strive for excellence
8. We will work as one team, always seeking new and better ways to deliver the best possible service for the public. We will be efficient and responsible with tax-payers' money.

1.5 Equality and inclusion

The CPS are proud to be recognised as a leading employer, committed to supporting a diverse and inclusive workforce that reflects the community we serve.

The CPS commitment to inclusion and equality is at the heart of how we work, underpinned by The Equality Act 2010 and Digital Accessibility standards. It is important to us both as an employer and in the way we approach our responsibilities as a prosecuting authority. The two are closely linked – supporting a diverse workforce allows us to provide a better service to the public.

We also value the insight we get from engaging directly with the communities we serve, who provide welcome scrutiny of our work. This inclusive approach means that:

- Effective community engagement builds greater trust with the public, higher victim and witness satisfaction, and better-informed prosecution policy and practice
- The CPS has an inclusive culture, reflected in a diverse workforce, locally and nationally, and at all levels of the organisation
- By opening up the CPS and acting on input from diverse communities, we aim to inspire greater confidence in our work, in particular from witnesses and victims, resulting in improved prosecution outcomes.

We are proud to employ and support people with physical and neurodiverse conditions. We hold ourselves and our suppliers to high Digital Accessibility Compliance standards to ensure all users are empowered to work efficiently, regardless of differences, to the same standard as people without these conditions. Our commitment to Accessibility by Default is demonstrated by embedding requirements within all aspects of CPS.

1.6 Why Work with CPS

Impacting on Criminal Justice: The CPS is responsible for delivering justice through the independent and effective prosecution of crime, as the principal prosecuting authority across England and Wales. We have a clear mission to make sure that the right person is prosecuted for the right offence, and to bring offenders to justice wherever possible. Working as supplier for

CPS opens opportunities for your organisation to play a key role in achieving these outcomes and enhancing the service we provide to victims and witnesses of crime.

Promoting opportunities for cross justice working: The CPS is at the heart of the Criminal Justice System. It is vital that our digital systems and processes operate effectively with those of our criminal justice partners, in the police, His Majesty's Courts and Tribunal Service, the defence community, the independent bar and with the judiciary.

Working with a world leading prosecuting authority: His Majesty's CPS Lead Inspector recently indicated that he considers CPS to be the leading Prosecution agency in the world. In particular, we consider that we are the most digitally advanced and we regularly give presentations to other prosecuting authorities in other countries to demonstrate the way in which we have used technology to digitise our systems. Working as a supplier for CPS opens opportunities for your organisation to be at the forefront of an internationally respected prosecuting authority.

Making an impact: As an organisation CPS is large enough to make a real difference across the CJS, and yet small enough for our suppliers to be key strategic partners. Working as a supplier for CPS, you will be presented with a range of interesting problems to tackle.

Committed to breaking boundaries: The CPS is heavily invested in developing our digital capability as an integral part of our CPS 2025 Strategy. We have launched exciting initiatives aimed at increasing our use of innovation and developing the casework tools that we will use in the future; are committed to delivering new core ICT, and to securing our data and unlocking its value. Working as a supplier for CPS opens opportunities for your organisation to be at the leading edge of this preparation for our future.

Ensuring the security of our data: The data we hold is one of our key assets and maintaining the trust of all our data subjects is crucial to maintaining public confidence. Working as a supplier for CPS opens opportunities for your organisation to work closely with us on privacy / security by design and to showcase how your ideas could improve the service we provide to those who trust us with their data.

1.7 Overview the ICT landscape

In the last 6 years we have made great strides in modernising our workplace. For example, regarding printing, we have reduced from 250 million sheets of paper per year in 2016 down to <50 million today.

During the pandemic, the CPS ensured effective use of technology internally and across the criminal justice system, using this as a positive catalyst for change, with benefits to operational business, communication, and wellbeing.

Our successful digital strategy and willingness to learn and adapt has been key, as highlighted in the HMCPSI report on the CPS response to Covid-19. "Not one member of staff we interviewed highlighted concerns about not being able to work because of not having access to the right IT kit."

Remote working: Like most of the world, CPS adapted from an office/Court based workforce to a home working/skeleton court-based workforce overnight. We have increased from 500 employees working from home per day to over 5000 who with thanks to our scalable infrastructure, and adoption of Microsoft teams, have been fully digitally supported.

CMS : Our prosecutors use a system called Case Management System to manage and progress case. Section 2 and 3 describe CMS and its associated systems. CMS currently contains approximately 5 million case records. At any one time the live case load of around 165,000; typically 450,000 case prosecutions per annum where 100,000 will be Crown Court cases.

Virtual hearings: One of the huge successes of the pandemic was the almost overnight launch of Court video hearings. In the past, Court hearings have largely been held on a physical basis, with virtual criminal hearings seen as many years away. 'Virtual court rooms' were set up on HMCTS' Cloud Video Platform (CVP) and allocated to physical courtrooms so participants appearing by video and those in the physical court room can participate in the same hearing.

Multimedia evidence: Over the previous two years the CPS has worked with the 43 police forces nationally to share multimedia digitally as part of their "war on disks". During the pandemic, where police forces continued to share around 1000 CPS discs per day, we used our own digital platform to provide disc-free access for prosecutors, defence, and judiciary, which is believed to be the first justice system in the world to achieve this. Of the 44 forces 33 have procured a DEMs solution and are in differing stages of usage and delivery. In terms of the other 11 forces again these at varying stages with some currently are going through a tender process now or working on the business case but we understand they there are some forces yet to have started on this journey.

New laptops: In 2020 the roll-out of new laptops for all staff commenced, replacing Lenovo machines with Microsoft Surface laptops running on a Windows 10 operating system with enhanced speed, longer battery life and easier portability. We were also able to donate 6,500 decommissioned laptops to UK school children to help them undertake virtual learning during the height of the pandemic.

ICT team: The team responsible for managing technology with CPS, has evolved in the last six years from managing a limited range of suppliers providing the majority of the technology to a structure which includes increased in-house management of core services.

2. CONTRACT SCOPE

There is a requirement to continue to administer, maintain and develop the CPS core casework applications and the supporting environment, and some other infrastructure items required by the CPS, before the current applications and hosting ("**A&H**") services contract expires in 2025.

In addition to providing this business-as-usual service, the Supplier of this ADIMS Contract will be required to work with one or more suppliers and internal CPS IT specialists to evolve CPS applications to a future state.

The overall contract will include below but not limited to:

- Support of CMS, WMS and MIS applications as currently implemented, and any other technology required to ensure these systems continue to operate as required by the CPS
- Vulnerability management and maintenance to ensure that the applications and underlying technology remain secure
- Resolving bugs in accordance with a prioritised list provided by the CPS
- Any changes required to ensure CPS adhere to legal requirements and the CPS's Standard Operating Procedures (SOPs), or as otherwise required by the CPS
- Secure decommissioning of data where required
- Working with other suppliers and delivering changes as CPS evolves the Future Casework strategy to deliver modern user-focussed applications to its users

The Supplier of this ADIMS Contract will provide appropriately skilled resources to run and maintain the legacy systems ensuring business continuity of the CPS's mission critical systems. This supplier's team will need to make changes to the legacy system to keep pace with change, including but not limited to new legislation and criminal justice procedures.

There will be a parallel contract to implement a new cloud-based infrastructure that will enable the current database environment to be re-platformed in due course. New services will interface with the re-platformed database, this will incrementally reduce reliance on the legacy system until it is fully replaced.

A further contract will be let to design and implement new core middleware services which will remove the business logic from the database, and to develop a user interface. Multiple suppliers will work together to an agreed design. This will be a combination of internal CPS capability, a multi-vendor panel and one of more third-party suppliers.

For the avoidance of doubt, the CPS will be referred to as the Buyer throughout this document.

2.1 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 Buyer Business Areas. CMS is the Buyer's business critical application supporting the core business process of prosecuting criminal cases. It is a national case tracking and management system providing case management for criminal cases dealt with in the

Magistrates', Crown, Appeal and Supreme courts. It supports the prosecution process by helping users manage the progress of a case throughout its lifecycle from receipt of a request for initial charging advice to the conclusion of a trial and post-trial activity such as appeals and proceeds of crime applications.

There are approximately 6,000 users of CMS. The application employs a browser-based architecture using Microsoft Edge in Internet Explorer 11 compatibility mode, DHTML, JavaScript and Microsoft 365 Apps for Enterprise at the client side.

CMS consists of 3 user interfaces sharing the same application platform. These are referred to as CMS Classic, CMS Modern and the Prosecutor App.

The ability to generate structured PDF electronic document bundles from case documents held in CMS is provided by Adobe Experience Manager (AEM). Functionality supporting users to email case information from within CMS is also available.

Physically all tiers of the core application and the structured bundling application are implemented within the ARK data centres. The client browser is provided on all Buyer laptops, and external users will provide their own compatible browser. The infrastructure makes use of VMWare 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 Buyer periodically requires CMS functionality updates, and these are implemented by releases throughout the year. The primary drivers for these changes span the following areas:

1. legislative changes to the way the Buyer operates
2. business optimisation of processes within the Buyer, including user-led efficiencies
3. changes to enable the Buyer 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.

2.1.1 CMS Key Functions

Information Capture – the CMS provides 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 Buyer 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 the Unique Reference Number (URN).

Assisted Production of Outputs – the Buyer produce a series of documents for presentation to the courts, the defence, the police and for use by the Buyer 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 Buyer 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.

2.1.2 CMS Processes

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)

Please refer to the Reference section for documents

2.2 WMS

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 staffed by Police and there are approximately 1,500 Users of WMS. Some of the units are connected directly to the Buyer network infrastructure whilst others are part of the police infrastructure.

The WMS application is made available to users across the Buyer network and to police users via the PSN network. The Police users access the WMS web site across their own force networks and then ultimately through their gateway onto the PSN. To provide further access controls on the sensitive information held in WMS a two-factor authentication mechanism for police users has been implemented using the HID ActivID technology.

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

2.2.1 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.

2.3 MIS

MIS (Management Information Systems) provides statistical and summary information on the progress of cases within Buyer. 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.

2.4 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 Criminal Justice System Exchange (CJSE) that allows for the exchange of information between CMS and the police case management systems and in the future other evidence gathering agencies.

The specific screens and supporting code to effect an enhancement to the interface to the Police are referred to as Digital Case File (DCF)

b. An interface to the Ministry of Justice (MoJ) Digital Case System (DCS) from CMS 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.

d. A set of interfaces to the Common Platform as per the table below. This is an in-flight programme

Interfaces	**Brief Description**
Service of Materials	The service of all case materials required
Unused Materials	Interface for Prosecutors to publish unused material schedules and disclosable material
Defence Disclosures	Publish defence disclosed material and defence statement to Buyer.
Application Request	This is API through which the Buyer will make applications to the court.
Application Response/Result	This is the mechanism through which information about relevant applications is sent to the Buyer
Case Directions In	Send updates on case directions with participants (including the CPS) via an interface
Case Directions Out	Receive updates on case directions with participants (including CPS) via an interface
Notices and Orders	Make outcome data available via interface

Further details on Interfaces are provided in the documentation set providing functional and technical documentation of CMS, WMS and MIS. Both Common Platform Interfaces and Digital Case File are in-flight projects and updates details will be provided at 3-month intervals. There is also an in-flight project to archive 2.9 million cases to a newly created CMS Archive.

3. FUNCTIONAL REQUIREMENTS

The Supplier is required to provide functional support for CMS, WMS and MIS. CMS, WMS and MIS have been developed specifically for the Buyer and needs to be provided exactly as set out within the functional specifications referred to in this Schedule.

The Supplier is required to additionally manage and support the systems and services which directly support the use of CMS; these are documented in the next section entitled Supporting Infrastructure:

The Buyer is responsible for managing the hosting of the virtual server environment for CMS, WMS and MIS and its associated systems and services, which reside in Crown Hosting Ark Data centres.

General Requirements

Reference ID	Requirement
GREQ001	CPS follows the Technology Code of Practice Service Standard on www.gov.uk – Service Manual.
GREQ002	The Supplier shall deliver all Services in accordance with the Contract, including the Standards
GREQ003	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 Buyer (e.g., operating models based on TOGAF (The Open Group Architecture Framework), and ITIL (Information Technology Infrastructure Library)).
GREQ004	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.
GREQ005	The Supplier shall wherever possible use simplified assurance and payment processes when invoicing the Buyer.
GREQ006	Save as otherwise expressly stated in the Call Off Contract, the Supplier shall ensure that, upon request from the Buyer, certain of: (i) the Supplier's Personnel; (ii) and any of the Key Supplier Personnel; and/or (iii) other relevant persons identified by the Buyer that the Buyer wishes to meet, shall attend workshops or meetings with the Buyer and/or any

Reference ID	Requirement
	other Related Supplier as the Buyer reasonably deems necessary given the circumstances.
GREQ007	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 Buyer of such failure or likely failure.
GREQ008	The Supplier shall notify the Buyer when it becomes aware of an actual or potential event that may pose a risk to the Services and shall provide to the Buyer all necessary details and information of such event.
GREQ009	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 Buyer.
GREQ010	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 Policy and Processes (PPs) would be subject to Schedule 5 (Change Control Procedure).
GREQ011	The Supplier shall perform the Services in accordance with Clause 7/8 of the Call Off Terms and this Schedule. The Supplier shall use the ITIL based processes documented by the Buyer and perform the Services in accordance with industry based best practice and, if required, the Supplier shall demonstrate this to the satisfaction of the Buyer.
GREQ012	The Supplier shall be provided with licences to use the ITSM Toolset, Service Now, 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 Schedule 5 (Change Control Procedure).

Reference ID	Requirement
GREQ013	The Supplier shall ensure that Processes for all ITIL functions are aligned (to the work instruction procedural level) with the Policies and Processes set out by the Buyer 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 Buyer, (ii) the Supplier and the Buyer; (ii) the Supplier and Related Suppliers are clearly set out in the Standard Operating Manual (SOM). Amendments to such Policies, Processes and Procedures that result in a material change to the Supplier Solution shall be subject to Schedule 5 (Change Control Procedure).
GREQ014	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 Buyer.
GREQ015	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 Buyer in advance.
GREQ016	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 Schedule 5 (Change Control Procedure).
GREQ017	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.
GREQ018	The Supplier shall ensure that all necessary support is provided to the Buyer, or any Auditor assigned or appointed by the Buyer, to audit any aspect of the Services provided by the Supplier.

Reference ID	Requirement
GREQ019	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 Buyer within thirty (30) Working Days of each annual anniversary of the date of Achievement of the Final Operational Services Commencement Date.
GREQ020	The Supplier shall bear the cost of decommissioning, collection and disposal of Supplier Equipment.
GREQ021	The Supplier shall provide to the Buyer access for validation purposes to all raw data and access on demand to all the Supplier's reporting tools.
GREQ022	The Supplier shall provide a SOM in accordance with this Attachment 1 and Call Off Schedule 4 (Implementation Plan, Buyer Responsibilities and Key Personnel), and update it in consultation with the Buyer from time to time and baseline it annually on each anniversary of the Call Off Commencement Date. The Buyer will provide a copy of the existing SOM for reference and as part of the handover.

3.1 Section 1 - Applications (CMS, WMS, MIS)

3.1.1 General Case Facilities

Reference ID	Requirement
APPS/R/GCASE/001	The following will apply to the functional specifications in this Section 1: • The Supplier will provide CMS / WMS / MIS functionality in accordance with the Functional Specifications named in the Virtual Data Room (VDR) at the time of Request for Proposal (RFP) issue. The Supplier and the Buyer 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. The Buyer will update the VDR periodically with the most up to date documents.
APPS/R/GCASE/001A	The Supplier shall deliver the functionality as set out in the detailed functional specifications: • 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

Detailed Functional Specification

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

a. CMS FS Cases subsystem (Refer to Reference section)

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

3.1.2 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 Buyer. The Supplier shall deliver the functionality as set out in the documents in the reference section:

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.

3.1.3 Reporting

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 Buyer. The Supplier shall deliver the functionality as set out in the reference section

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.

3.1.4 WMS Manual Entry

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

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.

3.1.5 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 Criminal Justice Organisation (CJO) systems and others including:

a) Police, (local and national forces);

b) Courts, Crown and magistrates' courts;

3.1.6 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

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 Buyer (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 Two-Way Interface (TWIF) enables the use of the Digital Case File (DCF). The DCF is a joint police and CPS initiative to improve and streamline the sharing of case information between policing and CPS. This replaces hand-filled and scanned documents with structured data. DCF is currently under development and is expected to be implemented from summer 2023.

The 1st version of the interface continues to be supported, thereby allowing Police forces flexibility in their implementation of changes yet will almost certainly be decommissioned during 2024 at the latest.

3.1.7 Courts Interface

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

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. Please refer to Reference section. This document is owned by a third party; Netmaster.
b. the second is to the CMS API for inbound from DCS to CMS. Please refer to the reference section.

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 114.doc>. This document is owned by HMCTS.

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

3.1.8 Interface with Common Platform

Refer to Common Platform CPS External API Specification

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

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

3.1.9 Data Currency

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

3.1.10 CMS Environments

<table>
<tr><th>Reference ID</th><th>Requirement</th></tr>
<tr><td>APPS/R/CMSENV/001</td><td>The Supplier shall provide the following environments:
<table>
<tr><th>ENVIRONMENT</th><th>USAGE AND NOTES</th></tr>
<tr><td>Development</td><td>CMS Classic development server / code repository.
CMS Modern Dev environment is in Azure.</td></tr>
<tr><td>Integration</td><td>CMS Classic development integration work prior to system testing for various project streams and MIS.</td></tr>
<tr><td>System Test</td><td>CMS Classic System Testing and UAT for various project streams and MIS.</td></tr>
<tr><td>Performance Test</td><td>Performance Testing for CMS Classic and Modern.
This is Classic CPT and Modern Perf Test, which are linked by a common database.</td></tr>
<tr><td>Production</td><td>CMS Classic and Modern production systems.</td></tr>
<tr><td>CIN2</td><td>CMS Classic testing and training preparation by the Buyer ahead of CMS releases.</td></tr>
<tr><td>CIN3</td><td>Joint testing with police systems or other external systems such as Digital Case System (DCS), Criminal Justice System Exchange (CJSE), Court Store, C2I/Common Platform etc.</td></tr>
<tr><td>CIN4</td><td>CMS Classic and Modern User Acceptance Testing (UAT) and system regression testing including Modern elements.</td></tr>
<tr><td>CIN5</td><td>UAT and demonstrations by the Buyer.</td></tr>
<tr><td>Model Office</td><td>Used by the Buyer for training using both CMS Classic and Modern.</td></tr>
</table></td></tr>
</table>

Reference ID	Requirement	
	CMS Archive	There is an archive of the CMS records, which is in place to retain data to be available for a number of public enquiries.

3.2 Section 2 – Supporting Infrastructure

The Supplier shall manage and support the following which a directly required to ensure the operation of CMS, WMS and MIS. Further technical detail will be provided on Servers (Windows and Linux), a 6TB Oracle RAC Database and other components e.g. Adobe Experience Manager which are used to 'bundle' documents for cases in PDF format.

The following items are also required to support CMS but are more in a peripheral role to the core system.

3.2.1 Windows AD

A Windows AD environment will remain within the Crown Hosting Ark Data centre to support the use of CMS. Its use is for managing and maintaining the Windows Servers.

Reference ID	Requirement
I1	The Supplier shall administer the Windows AD environment used to manage the Windows Server environment

3.2.2 DHCP & DNS

The Supplier will be required to manage the DHCP and DNS within the Ark Data centre. There are two DHCP servers that as a failover pair

Reference ID	Requirement
I2	The Supplier shall manage IP addresses, DHCP scopes and DNS within the environment including for the Linux servers used by CMS.

3.2.3 PSN Service

The Public Sector Network (PSN) service is in place to facilitate the exchange of information with police forces. At this time the message platform exchange (CJSE) service is still connected via the PSN. The Buyer also accesses a small number of web services such as JARD over the PSN.

Reference ID	Requirement
I3	The Supplier shall monitor and support the services used to provide links and connect to the Government PSN network

3.2.4 Internet access

Internet access is required for the Domain controllers to ensure they receive security updates. There are plans to phase out these proxy servers in 2023.

Reference ID	Requirement
I4	The Supplier shall administer the security configuration to allow a limited amount of access to the Internet as required to support the service.

3.3 Section 3 – Other Infrastructure

This section documents requirements intended to migrate from the current contract by end of 2024 but are retained in case there is a delay in the roadmap. This section will be updated at 3-month intervals to reflect the latest status. Further detailed technical detailed will provided.

The Supplier shall temporarily manage and support the following:

3.3.1 Windows AD

The Buyer plans to decommission the link between Windows AD (which will continue to be managed under this contract for the purposes of managing and maintaining Windows servers) and Azure AD (where Buyer management will commence once the link with Windows AD is removed).

Reference ID	Requirement
OI1	The Supplier shall support the Windows AD environment remaining from May 2025, providing support for the following items until they are decommissioned. The current dependency on Windows AD as follows 1. CMS authentication using Windows AD 2. WMS authentication integration using Windows AD to Azure AD, preferably with SSO. for police users) 3. Removal of some domain controllers from the DNS resolution path 4. Hermes integration – Hermes must be updated to integrate with Azure AD. 5. General file services authentication integration – this must be updated to integrate with Azure AD 6. ActivID – there may be some existing integration with Windows AD which might need to be change. 7. Service desk terminal servers and contingency terminal servers 8. Service dashboard

Reference ID	Requirement
	9. Petty France on-site servers 10. Exchange hybrid servers' replacement with new non AD-integrate MTA.

3.3.2 Buyer Site Wide Area Network (WAN)

This will be retained until replaced by a modular Wi-Fi solution and Ivanti Connect Secure or a similar solution will be retained until it is replaced by a point-to-multipoint solution. The implication of this is that significant ExpressRoute bandwidth will be required until the decommissioning is substantially complete, but we should look to ramp down the bandwidth, as the technical requirement decreases.

Reference ID	Requirement
OI2	The Supplier shall monitor and support any WAN connections terminating in datacentres.

3.3.3 Pulse Secure Services

The Buyer is reviewing the future roadmap of the Ivanti Connect Secure service with a view to replacing this system prior to the commencement of this contract.

Reference ID	Requirement
OI3	The Supplier shall monitor, administer and support Ivanti Connect Secure appliances and services.

3.3.4 HID ActivID Services

The Buyer plans is in the short term to scale down, and in long term to decommission ActivID, replacing it with a new solution for second-factor authentication.

Current main user groups are:

Buyer users – will be removed by completion of the EUC rollout project

Police users – will continue to need some authentication mechanism to secure their access to WMS. There is a potential to use a new Azure AD integrated hardware second factor, and/or Azure AD federation with police systems.

After full EUD rollout the Buyer expects ActivID will only be used for CMS/WMS over the PSN, but this requires verification.

Reference ID	Requirement
OI4	The Supplier shall monitor, administer and support HID ActivID Services.

3.3.5 NetApp ONTAP File Service

The Buyer intends to review the NetApp solution with possible view to replace it with a new file storage service. CMS files associated with cases are stored on this service. There is an in-flight project to tier the storage to Azure.

Reference ID	Requirement
OI5	The Supplier shall monitor, administer and support the NetApp devices.

3.3.6 Service Dashboard

The Buyer currently operates a Service dashboard using PRTG; it intended to bring this service in-house

Reference ID	Requirement
OI6	The Supplier shall monitor, administer and support the PRTG instance.

3.3.7 PKI Service

A Public Key Infrastructure (PKI) service is required to support the windows architecture.

Reference ID	Requirement
OI7	The Supplier shall monitor, administer and support of the PKI which supports the Windows architecture.

3.3.8 Contingency Terminal Services

It is intended to replace contingency terminal services with public cloud Virtual Desktop services.

Reference ID	Requirement
OI8	The Supplier shall monitor, administer and support contingency terminal services

3.3.9 Web proxies for use by datacentre devices

Web proxies are currently used by certain datacentre devices to access the internet.

Reference ID	Requirement
OI9	The Supplier shall monitor, administer and support web proxies

4. NON-FUNCTIONAL REQUIREMENTS

NFRs are the quality attributes for a system, as distinct from the functional requirements, which detail a system's business features and capabilities.

These requirements can have a substantial impact on solution development, testing and operation.

4.1 Security

Reference ID	Requirement
SE1	Supplier Personnel shall be subject to pre-employment checks and will ensure compliance with security clearance requirements prior to deployment of any staff onto the Buyer account, as outlined in the security schedule. Supplier personnel should ensure prompt notification of any change in personal circumstances, or when an employee has left, or moved away from Buyer work and no longer requires a security clearance. Changes in an employee's circumstances or new information obtained about employees which could have an impact on security clearance or suitability to operate in their role accessing the organisations systems should be reported to the organisation (e.g arrest/convictions etc) in a manner that is in accordance with data protection laws and regulations.
SE2	The supplier shall have in place an appropriate disaster recovery policy and process, including secure backup solutions, to maintain continuity and minimise downtime/impact to the Buyer in the event of an incident at the supplier side.
SE3	The supplier should be able to evidence the security of their network where any such systems access Buyer systems and data, or store Buyer data.
SE4	The Supplier shall ensure that the system is governed to NCSC standards but must provide audit data to comply with, or facilitate compliance with, the applicable requirements of the NCSC's Minimum Cyber Security Standard - GOV.UK (https://www.gov.uk/government/publications/the-minimum-cyber-security-standard). All accounting data shall be exported automatically by a standard method and held for a timeframe in line with agreed compliance and legislation. As a minimum the Supplier will need to be ISO27001:2013 certified, and Cyber Essentials accredited.
SE5	The Supplier shall provide the Buyer access to Supplier Staff and Supplier premises as required for the purposes of improving and auditing security. The Supplier shall make available to the Buyer and its designated agents any reasonably requested resources including physical access to the Site, facilities and Key Personnel that support the delivery of this requirement.

SE6	If any equipment or systems fall outside the scope of the Buyer estate, then the Supplier shall be responsible for the required IT Health checks/Penetration Testing to the satisfaction of the Buyer on an annual basis. All IT Health checks / Penetration Testing shall be delivered by a NCSC approved penetration testing service provider.
SE7	The Supplier shall ensure that access to all documentation, code and infrastructure is limited to authenticated and authorised supplier personnel only, with appropriated auditing mechanisms in place. These reports should be made available to the Buyer upon request.
SE8	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 Buyer Data. The Supplier shall control and monitor access to areas that could facilitate access to Buyer Data or services by physical access control mechanisms to ensure that only authorized Supplier Personnel are allowed access and maintain records aligned to ISO27000 certifications.
SE9	The Supplier shall deploy an effective authentication process for any devices to the network 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.
SE10	The Supplier shall deploy an 'incident response' arrangement that aligns with wider response procedures in place across the Buyer ICT Environment.
SE11	The Supplier would be expected to deliver a Security Management Plan in line with the Services delivered by the Supplier as part of the Contract. This should be reviewed annually by Supplier & Buyer and mutually agreed.

4.2 Availability

The Buyer's Policy and Process related to Incident Management has been provided in the data room as part of the Buyer's tender documentation

The Supplier shall adhere to the Buyer Service Operations – Availability and Capacity Policy & Process.

The Buyer's Core hours are 7:00 am – 7:00 pm (Monday – Friday) and Saturday 7am to 12noon. However prosecutors do prepare for cases outside core hours.

There is a 24x7x365 operation provided by CPS Direct (CPSD), for the purposes of making Charging decisions, and Services provided by this Contract must be supported for CPSD use.

The Buyer seeks to minimise Unplanned and Planned downtime.

Reference ID	Requirement
A1	The Supplier will be responsible for the availability of the Services. The Services are expected to be available 99.9%. This is defined in the Service Level schedule. This excludes planned downtime.

4.3 Digital Accessibility

Assistive Technologies

Around 15% of users are known to operate with assistive technology such as software, additional hardware and peripherals. This includes, but is not limited to:

a. JAWS
b. Dragon
c. ZoomText
d. TextHelp
e. Mind View
f. StreamDeck
g. Joystick mouse
h. Foot mouse
i. One handed keyboard (limited F keys) and external screen overlays.

As a standard, the Buyer expects that all new services and systems are compatible with assistive technology and meet the Government Digital Accessibility requirements. See Understanding accessibility requirements for public sector bodies - GOV.UK (www.gov.uk).

Reference ID	Requirement
DA1	The supplier shall ensure all new aspects and elements of services meet the Web Content Accessibility Guidelines (WCAG) 2.1 AA as a minimum, at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA2	The supplier shall ensure all new aspects and elements of services meet the Buyers compliance auditing standards, at all times. Any

Reference ID	Requirement
	exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA3	The supplier shall ensure that all new screen and changes to any existing screens within the current solution must meet the WCAG 2.1 AA as a minimum at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA4	All training and communications provided by the Supplier must meet WCAG 2.1 AA as a minimum and the Buyer's compliance auditing standard, at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA5	Any workarounds to meet WCAG 2.1 AA and or compliance auditing standards, must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA6	Any workarounds to meet WCAG 2.1 AA and or compliance auditing standards, must have a resolution plan agreed by the Buyer's Digital Accessibility Compliance Team, and be implemented at the pace agreed.
DA7	The Supplier shall triage and direct contacts from Digital Accessibility users to the resolver teams as directed by the Buyer's Digital Accessibility Compliance Team.
DA8	The supplier shall provide an accessibility statement before any type of go-live, including transition, launch, change and be reviewed at least annually.

4.4 Service Operations

Reference ID	Requirement
	The Supplier will be provided with access at appropriate levels to the Buyer's provided ITSM (Service NOW), which will also be accessed and updated by the Buyer and Other Supplier support teams. The Buyer's ITSM will be used by the Supplier to manage the following processes and all functions will be recorded in the ITSM. • Incident Management & Major Incident Management • Problem Management • Service Level / Priority Management • Change Management

	• Service Asset and Configuration Management • Request Fulfilment Management • Event Management • Access Management • Knowledge Management • Continuous Service Improvement • Service Level and MI Reporting • Buyer Satisfaction • IT Service Continuity Management • User Account Management (UAM) The ITSM (which will be "ServiceNow") will be made available to the Supplier by the commencement of Implementation.

Based on the pre-existing SOM (Service Operation Manual), the Supplier will produce their own SOM as part of on-boarding activities, as requested above.

4.4.1 Incident Management & Major Incident Management

Incident management is an ITSM process area. The first goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

The Buyer's Policy and Process related to Incident Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

The Supplier shall adhere to the Buyer Service Operations Incident Management Policy & Process.

Reference ID	Requirement
I1	The Supplier shall implement Incident logging procedures (which adhere to the Buyer's Policy and Processes (PPs)) with the Buyer and the other suppliers during the Implementation phase.
I2	The Supplier's Solution should allow Incidents to be detected (or identified) in a variety of ways, including but not limited to: a. the Event Management process. b. Supplier's or Other Supplier's monitoring activities. c. Availability management processes. d. Capacity Management processes (e.g., events from servers managed by Other Suppliers may result in the registering of an Incident); or e. by the Buyer's technical staff or Users.

Reference ID	Requirement
	Irrespective of how an Incident is registered, the Supplier shall record and hold such information to allow subsequent activity to take place to resolve the Incident.
I3	The Supplier shall use the Buyer's Incident management procedures to determine: a. The Incident category and subcategories. b. The priority to be associated with the Incident. c. The Resolver Group to which the Incident needs to be allocated.
I4	The Supplier shall agree any changes to the Policy or Processes used with the Buyer, prior to implementing any such change.
I5	The Supplier shall accurately record all Incident Management data within the ITSM ServiceNow.
I6	The Supplier shall ensure that each Incident once recorded, is associated with the relevant Service Level within the Buyer's ITSM tool (ServiceNow)
I7	The Supplier shall ensure that each Incident, once recorded, is associated with any existing Known Errors, Problems or other Incident records to support a potential first time fix or aid escalation to the relevant Resolver Group.
I8	The Supplier' shall assign the required time to fix to the Incident record, and the Supplier shall advise the User of the anticipated fix time.
I9	In the event of a dispute as to the Severity Level assigned, the matter shall be escalated within the Supplier's and the Buyer's organisation
I10	The Supplier shall ensure the ITSM is used to track the elapsed time during the life cycle of the resolution and shall create alerts at predetermined points set out in the SOM. The Supplier shall use this information to monitor the progression of each incident and escalate appropriately with the Resolver Groups.
I11	The Supplier shall use the ITSM so that Incidents are automatically escalated to the Supplier's management at pre-determined points, based on the time that has expired since the occurrence of notification of the incident. The escalation processes shall include procedures for exception reporting to the Buyer.
I12	The Supplier shall validate the User's profile and entitlement to service upon a User recording an Incident at the earliest opportunity.
I14	The Supplier shall own the records for all Incidents and be accountable for their progression throughout the ITIL Incident life-cycle.

Reference ID	Requirement
I15	The Supplier shall provide feedback to Users 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; and (iii) advice allowing the User to continue to use the Services until such time as the Incident is Resolved.
I16	The Supplier shall adhere to the Buyer's PP's with respect to Incident closure and re-opening.

ITIL defines a special process for dealing with Major Incidents (emergencies that affect business-critical services and require immediate attention). Major Incidents typically require a temporary Major Incident Team to identify and implement the resolution.

The Buyer's Policy and Process related to Incident Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

The Supplier shall provide a Major Incident lead / escalation point for P1 & P2 type of incident.

Reference ID	Requirement
M1	All Severity Level 1 and Severity Level 2 Incidents shall be defined as Major Incidents. The Supplier shall work with the Major Incident manager to support the process of resolving the incident.
M2	The Supplier shall provide a point of contact for the Buyer Service Management Team for escalation and information purposes during the lifecycle of the Major Incident.

4.4.2 Problem Management

Problem Management is the process responsible for managing the lifecycle of all problems that happen or could happen in an IT service. The primary objectives of problem management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented. ITIL defines a problem as the cause of one or more Incidents

The Buyer's Policy and Process related to Problem Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
P1	The Supplier shall work with the Buyer and Other Suppliers to define and implement the criteria for prioritisation of Problems.

Reference ID	Requirement
P2	The Supplier shall maintain Problem Management records using ServiceNow.
P3	The Supplier shall ensure that Problem records contain the following details as a minimum: a. Date and time of Problem raised b. Relevant dates and times of occurrence of any Incidents c. Category d. Business impact/urgency e. Resultant priority f. Actions taken/history/timings g. Links to resultant Incidents h. Name of person who made the modification i. Date and time of modification j. What the person modified (e.g. priority, status, history) k. Why they made the change l. Next actions and timescales m. Details of any interaction with the Buyer n. Links to relevant knowledge management articles o. Supplier who owns the problem investigation.
P4	The Supplier shall ensure that Problem Investigation is carried out typically for: a. Incidents for which the root cause is unknown b. All Major Incidents c. For Incidents which have been repeated or where there are indications that they are likely to be repeated.
P5	The Supplier shall retain overall responsibility for recording and tracking Problems until the Problem is closed.
P6	The Supplier shall allocate Problems to Other Suppliers or a Resolver Group as appropriate.
P7	The Supplier shall progress all activities required to diagnose the root cause of Major Incidents and Problems and to determine their resolution.
P8	On the Buyer's reasonable request, the Supplier shall undertake all activities required to diagnose the root cause of all problems and to determine their resolution.
P9	The Supplier shall co-ordinate the effective execution of Problem investigation and diagnosis across Other Suppliers to identify the fault in the Service that caused the Problem.
P10	The Supplier shall recommend to the Buyer measures to prevent the recurrence of all Problems.

Reference ID	Requirement
P11	The Supplier shall initiate action to negate or eradicate where possible the root cause of all Problems, such actions to be agreed with the Buyer.
P12	The Supplier shall record Known Errors and their Workarounds or Problem resolutions in the ITSM.
P13	The Supplier shall conduct Problem Management meetings as required by the Buyer, to prioritise the resolution of Problems.
P14	The Supplier shall maintain regular communications between all relevant parties until Problem resolution is achieved.
P15	The Supplier shall escalate to appropriate management within any Other Supplier's organisation structure if corrective actions are not being progressed.
P16	The Supplier shall document and publish Problem Management meetings status reports to the Buyer and to Other Suppliers.
P17	The Supplier shall receive Problem Management information on a monthly basis from Suppliers and produce trend analysis and management summaries to identify trends, significant changes or increases in Problem volumes for discussion with the Buyer and Suppliers at the appropriate forums.

4.4.3 Change Management

Change Management is an ITSM discipline. The objective of change management in this context is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in the IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g., legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives, including for digital accessibility.

The Buyer's Policy and Process related to Change Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
C1	The Supplier shall adhere to Buyer PPs. and, where requested, contribute effort to requests which require Changes across the Multi-Supplier Operational Environment.

Reference ID	Requirement
C2	The Supplier shall take all such actions as required to enable the Buyer to respond to urgent requirements for Change, as set out in Schedule 5 (Change Control Procedure) and in the Change process Policies and Processes (PPs).
C3	The Supplier shall provide the flexibility to “fast track” certain Changes, where urgent requirements for Change have been identified by the Buyer. Schedule 5 (Change Control Procedure) articulates the process for handling such Change.
C4	The Third party shall discuss with the Buyer before implementing any change. Prior notice is required.
C5	The Supplier shall adhere to the Buyer Service Operations – Operational Change Management Policy & Process.
C6	The Supplier shall adhere to the Buyer Service Operations – Commercial Buyer Change Management Policy & Process.

4.4.4 Operation of a Service

The Buyer’s Policy and Process related to Operation of a Service has been provided in the data room as part of the Buyer’s FCT ADIMS tender documentation.

Reference ID	Requirement
OSD1	The Supplier shall ensure all components that make up the Services continue to be of sufficient capacity to meet the Buyer’s operational needs. This includes providing sufficient capacity to cater for growth in use over the Contract Period.
OSD2	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 Buyer b.The Supplier shall not withdraw any service for any reason without formal Approval by the Buyer. c. All outages shall be confined to the Outage Window as agreed by the Change Advisory Board. d.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 Buyer.

Reference ID	Requirement

4.4.5 Service Asset and Configuration Management

The Buyer's Policy and Process related to Service Asset and Configuration Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
S1	The Supplier shall contribute asset record data to a master CMDB within the (Buyer provided) ITSM tool (ServiceNow) for the recording of hardware and software assets supported under this Contract.
S2	The Supplier shall maintain the CMDB records (on behalf on the Buyer) to include all the information as set out in the relevant Buyer Policy and process documents, including but not limited to: a. whether a CMDB item is considered out of support. b. the End of Life date; and c. warranty period.
S3	The Supplier shall provide regular software and hardware asset reporting to the Buyer. The format and frequency of these reports will be agreed during Implementation and set out in the Service Operation Manual.
S4	The Supplier shall ensure that the master CMDB is updated at regular intervals to be agreed during Implementation.
S5	The Supplier will continue to coordinate from other suppliers any changes that need to be made to the master CMDB. The frequency of this task to be agreed during Implementation.

4.4.6 Request fulfilment management

The Buyer's Policy and Process related to Request fulfilment Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
R1	The Supplier shall respond to requests originating from the ITSM Service Catalogue in accordance with the Buyer Policy and Process documentation relevant to Service Requests management. Catalogue items include the following in addition to a set of service requests for CMS:

Reference ID	Requirement
	• Firewall Rule Update, • DNS Entry, • Pulse Split Tunnelling, • Add or Remove AD Group - only for CMS Service • Technical staff call off - Rate card - not for incidents, • Site Closure (Decommission Buyer Site) - needed to tidy DCHP, • Site Move, • Simple Service Desk Script Updates
R2	The Supplier shall review management reporting information on a monthly basis to identify trends or significant changes or increases in Service Request volumes, for discussion with the Buyer.
R3	The Supplier shall identify possible process improvements and promptly make appropriate recommendations to the Buyer.
R4	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Service Desk in response to Service Requests.
R5	The Supplier shall proactively manage and monitor the status and progress of fulfilling Service Requests.
R6	The Supplier shall respond to the Buyer's enquiries regarding Service Requests with accurate and up-to date information

4.4.7 Event Management

The Buyer’s Policy and Process related to Event Management has been provided in the data room as part of the Buyer’s FCT ADIMS tender documentation.

The Supplier should provide pro-active monitoring and then raise incident

Reference ID	Requirement
E1	The Supplier shall assist the Buyer in establishing and implementing effective end to end Event Management.
E2	The Supplier shall assist the Buyer to ensure that Events are effectively managed in accordance with the required outcomes, e.g., identifying the events that are turned into Incidents and allocating them an appropriate priority.

4.4.8 Access Management

The Buyer's Policy and Process related to Access Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
AC1	The Supplier shall be aware that it will service request for access to CMS, WMS and MIS from the Service Catalogue. These will need be actioned promptly, according to Service Levels.

4.4.9 Knowledge Management

The Buyer's Policy and Process related to Knowledge Management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
K1	The Supplier shall capture details of Known Errors as soon as they are known and record it in the ITSM in the ServiceNow knowledge base

4.4.10 Continuous Service Improvement

CSI is concerned with ensuring that ITC services support business processes effectively and efficiently. The emphasis is on end-to-end service performance as opposed to component performance, and thus on the IT service as the Buyer experiences the service. ITIL identifies three basic measures of service performance:

- Availability of the service,
- Reliability of the service,
- Performance of the service.

Continual Service Improvement (CSI) planning focuses on service improvement that supports business processes. Our CSI uses a seven-step improvement process plan which is critical for itself and other stages of the ITIL lifecycle.

The seven-stage process is as follows:

- Identify the approach for improvement
- State what will you measure
- Collect the Data
- Process the data
- Analyse the data and information
- Present and use the information
- Implement corrective or remedial activities

The Buyer's Policy and Process related to Continuous service improvement has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
CS1	The Supplier shall review all of the Services on a regular basis in collaboration with the Buyer and, where appropriate, other relevant Suppliers, with a view to improving service quality and accessibility where necessary, and to identify more effective and efficient ways of providing the Services where possible.
CS2	The Supplier shall evaluate processes on a regular basis. Such evaluation to include identifying areas where Service Levels are not reached, holding regular bench markings, audits, maturity assessments and reviews.
CS3	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 Buyer's cooperation. Any such initiatives will require the approval of the relevant role within the Buyer's Service Management Team. Note to Supplier - Roles and responsibilities will be agreed as part of the Supplier on-boarding process.
CS4	The Supplier shall verify if improvement initiatives are proceeding according to plan and introduce corrective measures where necessary.
CS5	The Supplier shall foster a culture which allows Supplier Personnel to capture, prioritise and communicate ideas across their teams, allowing any Supplier Personnel to suggest innovative and accessible improvements.
CS6	The Supplier shall provide training, share best practise and enhance the knowledge of the end users on the I.T. service provided.

4.4.11 Service Level monitoring and MI reporting

The Buyer's Policy and Process related to Service Level management has been provided in the data room as part of the Buyer's FCT ADIMS tender documentation.

Reference ID	Requirement
SL1	The Supplier shall monitor Achieved Service Levels and compare them with agreed Service Level Performance Measures. This information shall be used as a basis for measures to improve service quality.

Reference ID	Requirement
SL2	The Supplier will provide Service Performance Monitoring Reports (with a preference for real-time data where available) that compare the Service Levels with the Achieved Service Levels, and include information on the usage of Services, ongoing measures for improvement of the Services, and any exceptional events that occurred during the period measured.
SL3	The Supplier shall use the ITSM to capture sufficient details to allow data to be extracted for the purpose of assisting in production of Service Management Reports for: (1) the Supplier's reporting against its Service Levels under this Call Off Contract. This should be presented in a legible format that is auditable. The data and reports shall be agreed during Implementation and shall include, but not be limited to: a. Details surrounding Incidents where the resolution of such Incidents has exceeded the Service Level Target relevant to the Incident Category assigned to the Incident. b. Where the failure to resolve an Incident within the Service Level Target relevant to the Incident, is a Repeat Failure, a progress report on the actions taken by, or on behalf of, the Supplier to Resolve the underlying cause and prevent recurrence. c. which Incidents have been Resolved and their Incident Resolution Times. d. which Incidents remain outstanding and the relevant Supplier's progress in Resolving them. e. reporting on aged Incidents
SL4	The Supplier shall use the ITSM to capture sufficient details to allow data to be extracted for the purpose of assisting in production of Service Management Reports. This should be presented in a legible format that is auditable. The data and reports shall be agreed during Implementation and shall include, but not be limited to: a. Details surrounding Incidents where the resolution of such Incidents has exceeded the Service Level Target relevant to the Incident Category assigned to the Incident. b. Where the failure to resolve an Incident within the Service Level Target relevant to the Incident, is a Repeat Failure, a progress report on the actions taken by, or on behalf of, the Supplier to Resolve the underlying cause and prevent recurrence. c. which Incidents have been Resolved and their Incident Resolution Times. d. which Incidents remain outstanding and the relevant Supplier's progress in Resolving them. e. reporting on aged Incidents
SL5	The Supplier shall ensure the data captured via the ITSM is timely and accurate such that other suppliers' reports relying on such data, accurately reflect the position at the end of the month.

Reference ID	Requirement
SL6	The Supplier shall provide reports and data on trends and root cause analysis to: A. allow the Buyer to make informed decisions. B. allow for pro-active management of issues

4.4.12 User Satisfaction, surveys and complaints

Reference ID	Requirement
CSS1	The Buyer will measure Buyer satisfaction by KPI.
CSS2	The Supplier shall, as a minimum, utilise their experience and expertise to recommend improvement actions required to increase User satisfaction rates.
CSS3	The supplier shall participate in collating relevant information and producing written responses to the Buyer in respect of User complaint

4.5 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 Buyer.

Reference ID	Requirement
CAP001	The Supplier shall monitor, analyse and report to the Buyer in relation to capacity volumes and trends and shall, where appropriate, act on any capacity related issues.
CAP002	The Supplier shall provide any reasonable information requested by the Buyer in respect of the Buyer overall capacity plan and support the on-going maintenance and development of such overall capacity plan.

Reference ID	Requirement
CAP003	The Supplier shall provide all such assistance as reasonably requested by the Buyer in establishing future capacity requirements for Supplier Systems, based on the Buyer's defined business needs and plans. The Supplier shall make recommendations to the Buyer 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.
CAP005	The Supplier shall provide standard Service reports which enable continual monitoring and insight into capacity trends. The Buyer shall review these reports to review capacity management on a monthly basis in liaison with the Supplier's technical resources.
CAP006	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.
CAP007	The Supplier shall manage, control and predict the performance, utilisation and capacity of IT resources and individual IT components (at a level to be agreed during Implementation).

4.6 Backup and Recovery

Background / Scope: A backup, or the process of backing up, processing data so it may be used to restore an original version from a certain set of points in time after a current instance of some data has been lost. The primary purpose is to recover data after its loss, be it by deletion or corruption.

Reference ID	Requirement
BREC001	The Supplier shall safeguard Software and Buyer Data against loss or damage. In particular, the Supplier shall: a. ensure that of all Software and Buyer data is available as the primary view was presented at a point between 23:00 and 03:00 every night for the 14 days prior to any request to make previous versions of data available.

Reference ID	Requirement
	b. make the most recent version, or any other version, of data available in the event of a loss of integrity of the current copy or for any other reason.; c. maintain a log of all events designed to protect data availability and integrity to enable speedy access and restoration maintain a log of all events designed to protect data availability and integrity to enable speedy access and restoration. d. provide all appropriate protection including up-to-date virus protection; and e. restore Buyer Data and user-specific applications upon request from a User, e.g. where a user has inadvertently deleted or corrupted Buyer data.
BREC002	In the event of the loss of a System, the Supplier shall ensure that Software and Buyer Data are fully restored to the state at the point of failure within the relevant Service Levels.
BREC003	The Supplier shall monitor and verify all backups at least on a daily basis. This will ensure that, in the event of system failure all 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. Records of the backup verification tests will be made available to the Buyer on request.
BREC004	The Supplier shall perform test restorations of production data from a recent backup copy at least once in each calendar year to prove that such data can be restored to a system. The restoration may be to a non-production system which is authorised to hold production data.
BREC005	On request by the Buyer, the Supplier shall restore the most recent version of Buyer Data to a point not exceeding one (1) Working Day previously.
BREC006	The Supplier shall ensure there is a redundant storage system such that the loss or failure of any one component of that system does not cause a loss of Buyer data. i.e. the data must be distributed over multiple storage devices with some kind of parity data generation. Also at least two copies of the data must be stored in locations at least 50km linear distance apart from each other.
BREC007	The Supplier Solution shall ensure that at least one copy is an off-site backup which is managed and stored in an independent manner from the installation in the Crown Hosting services.

Reference ID	Requirement
BREC008	The Supplier shall enable the transfer of valuable but seldom used Buyer Data to a cost efficient, reliable and secure repository, to migrate seldom accessed data to more cost effective storage solution.
BREC009	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 the Internet.

4.7 Proactive Monitoring

Reference ID	Requirement
PM1	The Supplier shall provide proactive monitoring on the services and applications (this will include monitoring of Servers, Database, Services, both for CPU and space reasons).
PM2	The supplier is expected to provide a performance monitoring tool for both the applications and the infrastructure. The Buyer will have access to the monitoring tool.

4.8 Change Programme Processes

From an overall change perspective, the Buyer requires that there are regular releases of the CMS software to address business as usual needs, and that all the underlying technical components are 'in support'. In order to achieve this the Buyer requires to work closely with the supplier to ensure there is an effective change programme in place.

Reference ID	Requirement
CP001	The Supplier shall work with the Buyer to create an agreed pipeline of change in all areas of the Service.
CP002	The Supplier shall develop changes and fixes for CMS in line with estimates, delivering in a timely manner.
CP003	The Supplier shall work with the Buyer on the forward maintenance plan for the infrastructure.

4.9 Working with other Suppliers

The Supplier will be expected to comply with the Collaboration Agreement schedule within the framework.

As mentioned in the introduction there will be a parallel contract to implement a new cloud-based infrastructure that will enable the current database environment to be re-platformed in due course as part of the Future Casework Tools Strategy.

Further contract{s} will be let to design and implement new core middleware services which will remove the business logic from the database, and to develop a user interface. Multiple suppliers will work together to an agreed design.

Reference ID	Requirement
WOS1	The Supplier shall actively work with other Suppliers as part of Ecosystem to improve performance, reliability, and stability
WOS2	The Supplier shall work with other suppliers on Triage of incidents as part of incident management
WOS3	The Supplier shall work with the appointed cloud-based infrastructure supplier, safely managing the integrity of the data as it is migrated away form this contract to the new platform.
WOS4	The Supplier shall work with the appointed user interface suppliers, which will also include working with in-house development teams to produce new user interfaces.

4.10 Update Documentation

Reference ID	Requirement
DOC001	The Supplier shall ensure appropriate functional and technical documents are updated after changes and shared with the Buyer as and when completed to maintain an up-to-date “Common View” at all times.
DOC002	The Supplier shall manage the update and maintenance of documents and codes in relation to the service / applications
DOC003	The Supplier shall produce Knowledge Articles and ensure Users’ experience is optimised and best practice is shared effectively.

5. FINANCE MANAGEMENT

The Finance team ensures the business runs efficiently by monitoring and keeping to best practise. It works to invoice and make payments promptly as per agreement. It ensures policies and processes are followed as described in the Charging Schedule.

Reference ID	Requirement
FM001	The Supplier shall produce a Monthly Service Performance Monitoring Report which shall be delivered within 5 Working Days of the Month's end.
FM002	The Supplier shall produce a monthly finance report which shall be delivered within 8 Working Days of the Month's end.
FM003	The Supplier shall comply with the current performance measurement, invoice / credit note process
FM004	The Supplier shall produce Service reports and Buyer shall approve if meets the set-out requirement before payments of Invoices are made
FM005	The Supplier shall send Future Demand Forecast on a monthly basis
FM006	Not used.
FM007	The Supplier shall be flexible and decommission from current contract and transition what we need as at when it is requested
FM008	The Supplier shall comply with, the relevant Standards within finance category in accordance with Good Industry Practice
FM009	The supplier shall provide transparency of its cost to support value for money.

6. SERVICE TRANSITION

The Buyers requires that Service Transition assurance to ensure that any new services, or changes to service, are assured as ready to move into Business-As-Usual. This includes ensuring that any required management and support documentation and processes are up to date and in place so the services can be effectively supported in the live environment.

Reference ID	Requirement
ST1	The Supplier will provide a Service Transition Manager during implementation of the contract to provide assurance of Transition activities and work with the Buyers' Service Transition Manager.
ST2	The Supplier will ensure that all Service Transition activity is planned throughout all phases of the Implementation and included in the Supplier Implementation project plans.
ST3	The Supplier will transition the services in line with ITIL good practice and the Buyers' Service Transition standards.
ST4	The Supplier will work with the Buyer to assure that all Service Transition activities are complete and documented in line with ITIL Service Transition principles.
ST5	The Supplier will engage with the Buyer Service Transition Manager about any potential changes to the service (including Charges) and agree the Service Transition approach at project initiation.
ST6	The Supplier will transition any changes to the services into the live environment in line with ITIL good practice and the Buyers Service Transition standards.
ST7	The Supplier will ensure that any new services or changes to existing services are approved by the Buyers Service Transition team prior to implementation in the live environment, and that any activities that need to be completed after go-live are agreed with the Buyer.
ST8	The Supplier will comply with the Buyers' Change Management process and provide all updates to the Buyers' Change Approval Board in line with the process.
ST9	The Supplier will work with the Buyers' Service Transition process in planning any exit or decommissioning activity.

7. IMPLEMENTATION & TRANSITION

As described in the relevant schedule for Implementation and Testing, the Supplier will be required to provide outline and detailed Implementation plans.

For guidance the Buyer expects the following three phases will be required in the Knowledge Transfer process, which is during the period before taking over the live operation of the contract:

- Information gathering phase: Working with the incumbent supplier there will be a process to discuss and understand the underlying documentation
- Test Phase: The Buyer expects to provide the opportunity to install a test CMS system using the documentation provided and with the support and assistance of the incumbent supplier.
- Production Phase:
    - The Supplier shall confirm they have all the required capability and access to prepare to manage the CMS, WMS, MIS applications and infrastructures.

Reference ID	Requirement
IT1	The Supplier will provide outline and detailed implementation plans as appropriate at stages of the contract tender.
IT2	The Supplier will work with the Buyer and Incumbent Supplier to achieve the successful handover, agreeing appropriate achievements through the Milestones.
IT3	The Supplier will apply their experience of providing similar services, to contribute to an effective, timely and successful takeover of the live services.
IT4	The Supplier will look to optimise value for money for the Buyer whilst balancing operational risk mitigation

8. MANAGED THIRD PARTY CONTRACTS SERVICES

Reference ID	Requirement
MPTC1	The Supplier shall manage and coordinate the activities of relevant third party suppliers of Managed Third Party Contracts in accordance with Attachment 5 (Key Supplier Personnel and Key Sub-Contractors). Such activities shall include, but not be limited to: a. maintaining technical support relationships with relevant with third party suppliers to resolve Incidents and Problems and to provide answers to technical questions and requirements related to the use of its products or services; b. monitoring relevant third party supplier service delivery and performance including third party supplier compliance with any performance indicators and target performance levels and report on such delivery to the Buyer on a monthly basis; c. providing consolidated compliance reporting for the monitoring and management of performance indicators and target performance levels, where the relevant third-party supplier is contractually required to provide compliance reporting data in a mechanised format; d. maintaining consistent use of reporting standards, formats, across Supplier, its Sub-contractors, and relevant third-party suppliers; and e. evaluating and recommending retention, modification, or termination of a third party supplier (and the relevant Managed Third Party Contract) based on the performance or cost benefits to the Buyer as tracked by the Supplier; such evaluation to be provided to the Buyer at the Buyer's request.
MPTC2	The Supplier will regularly maintain and propose updates to the Managed Third Party Contracts, as applicable, including: a. such updates to include Managed Third Party Contract list data requirements in sufficient detail as agreed between the Buyer and the Supplier to enable operational and commercial management of the relevant third party supplier's services; b. maintain the Third-Party Contract list as necessary to ensure that the information held is current and accurate; and c. propose updates to the Managed Third-Party Contract list whenever there is an addition or deletion of a Managed Third Party Contract; and

Reference ID	Requirement
	d. participate in a monthly contract review process with the Buyer.
MPTC3	The Supplier may use the Managed Third Party Contracts, as applicable, as necessary for the delivery of the Services and will: a. Liaise with and be the primary point of contact for the third party supplier for the purpose of answering questions, providing direction and resolving issues; b. Monitor and co-ordinate the services delivered by the third party supplier to verify compliance with the terms of the relevant Managed Third Party Contract; c. Accurately record delivery performance by the third party supplier in sufficient detail to support periodic renegotiation of contract terms by the Buyer and provide such as reasonably requested by the Buyer; d. Assist the Buyer to verify the accuracy of third party supplier invoices using the data from the delivery performance measurement system described above; e. Report third party supplier delivery performance to Buyer on a monthly basis and as requested by the Buyer from time to time; f. Promptly notify the Buyer of any non-compliant delivery by third party supplier; and g. In the event of third party supplier non-compliant delivery: - Initiate corrective actions as provided for in the terms of the Managed Third Party Contract; - Monitor the progress of corrective action taken by third party supplier; and - Update the status to the Buyer and keep the Buyer informed as to the status and resolution of third party supplier corrective action h. Promptly notify the Buyer of any disagreements or disputes, related to Supplier use of third party supplier's services for delivery of the Supplier Solution, to the Buyer for resolution; i. Report invoice validation data and results in a timely manner to the Buyer; j. Support the Buyer in Managed Third Party Contract negotiations as the Buyer reasonably requires; and

Reference ID	Requirement
	k. Advise and provide reports to the Buyer regarding Managed Third Party Contract strategy in order to optimise the Managed Third Party Contract list such as proposing consolidations and alternative sources of supply.

9. Software Licence and Asset Management

Reference ID	Description
SLAM1	The Buyer shall maintain and make available to the Supplier the Buyer's Software Asset Management Policies and Processes.
SLAM2	The Supplier shall comply with the Buyer's agreed Software Management Policies and Processes.
SLAM3	The Supplier shall work with the Buyer and the Other Suppliers to implement the Buyer's Software Asset Management Policies and Processes.
SLAM4	The Supplier shall administer, support and control the Software Asset Management Policies and Processes including the acquisition (where requested by the Buyer), documentation, distribution and installation, usage and retirement of software assets, in accordance with the relevant software licence agreements and in accordance with the Technical Framework Document.
SLAM5	The Supplier shall define and maintain Operating Procedures for Software Asset Management that are aligned to the Buyer's Software Asset Management Policies and Processes and the Technical Framework Document and shall submit them to the Buyer for approval.
SLAM6	The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Software Asset Management including but not limited to content creation, update, change control and circulation across Other Suppliers.
SLAM7	The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Software Asset Management and report such non-compliance to the Buyer.
SLAM8	Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Software Asset Management, the Supplier shall bring this to the Buyer's attention.
SLAM9	The Supplier will use the Supplier's IT Asset Management (ITAM) solution to support the agreed Software Asset Management Policies and Processes.
SLAM10	The Supplier shall, where there are gaps in the functionality of the Supplier's existing tools and software to support the Software Asset Management Policies and Processes, agree with the Buyer how these gaps will be addressed.

SLAM11	The Supplier shall provide and enter the data into the Buyer's specified ITAM solution for: a. purchasing of all software assets; b. optimisation of the software asset purchasing process; c. deployment of all software assets on the Buyer's estate; d. maintenance of the software assets on the Buyer's estate; e. monitoring the utilisation of the software assets; f. optimising the utilisation of the software assets; and g. tracking of licence expiration and advising the Buyer accordingly disposal of software assets.
SLAM12	The Supplier will work with the Buyer to minimise the costs associated with the deployment and operation of software assets by automating its processes wherever possible, in particular (though not limited to) those associated with inventory tracking, issue tracking, patch management, software deployment and configuration compliance.
SLAM13	Each Service Period, the Supplier shall review all licence deficiencies and provide a software licence compliance report in the format specified by the Buyer.
SLAM14	Each Service Period, the Supplier shall remediate any licence deficiencies identified in the software licence compliance report identified in Paragraph 12.3.14 above, which relate to any licences that the Supplier acquires on behalf of the Buyer, including any ITSM Product related licences.
SLAM15	The Supplier shall manage compliance with all Software licences by monitoring and auditing all Software use on behalf of the Buyer and in accordance with the Buyer's Software Management Policies and Processes and the Technical Framework Document.
SLAM16	The Supplier shall ensure that all necessary support is provided to any Auditor or any external licence audits requested by the Buyer or authorised third parties.
SLAM17	The Supplier shall provide appropriate auditing tools including software licensing in support of Software licence Management.
SLAM18	The Supplier shall proactively monitor the use of all Software in order to maintain strict compliance, such monitoring activities to include: a. immediately notifying and advising the Buyer of any Software licence compliance issues identified within the Buyer's IT Environment or associated with the use of or support of the Services provided to the Buyer; b. monitoring all software associated with the Services, ensure appropriate provisioning and availability of Software; c. ensuring appropriate monitoring is put in place for the purposes of identifying the presence of any unauthorised or non-standard Software; d. providing periodic reporting of license information and compliance to Buyer, as required; and

	e. filing and tracking Software license agreements in the Service Portfolio and ensuring appropriate links within the CMDB, the asset register and Definitive Media Library.
SLAM19	The Supplier shall, every six months following the Effective Date, undertake a review to identify any software currently in use which is not at the agreed release level and propose a strategy to Upgrade to the agreed release level.
SLAM20	The Supplier shall ensure that the CMDB is kept up to date with licence information in line with the relevant Buyer Policies and Procedures.
SLAM21	The Supplier shall maintain accurate and up to date records of all licences provided by the Supplier for use of the Services and of all licences for hardware and software used by the Supplier in the provision of the Services to the extent that such licences were maintained by the Supplier at the Effective Date.
SLAM22	The Supplier shall provide the Buyer with access to the records of such licences.

10. GLOSSARY

GLOSSARY	
Term / Abbreviation	**Explanation**
AD	Active Directory
ADIMS	Applications, Databases and Infrastructure Management Service
API	Application Programming Interface
Buyer	The Crown Prosecution Service (CPS)
CaaS	Change as a Service (CaaS) is a resource supply service that allows you to draw on external capabilities to improve your delivery, and to help you to meet your change needs. It's a service that delivers consistent and transparent change management. It significantly decreases your delivery risk and increases your ability to successfully deliver change. Any organisation looking to build a tailored change delivery platform can benefit from using CaaS.
CDA	Core Data API
CIN	C(MS) IN(tegration) test
CJSE	Criminal Justice System Exchange
CMS	Case Management Application is used by the whole of the CPS to progress cases and support the prosecution of cases. It consists of 3 user interfaces sharing the same application platform. These are referred to as CMS Classic, CMS Modern and the Prosecutor App.
CPS	Crown Prosecution Service, referred to as the Buyer in this document
DA	Digital Accessibility

DCS	Digital Case System
DHCP	Dynamic Host Configuration Protocol
DID	Digital and Information Directorate
DNS	Domain Name System
ERD	Entity Relationship Diagram
EUC	End User Compute
EUD	End User Device
FTE	Full Time Equivalent
HLD	High Level Design
LLD	Low Level Design
MBAM	Microsoft BitLocker Administration and Monitoring
MIS	Management Information System provides reports on business performance based on data extracted from the CMS database.
MWP	Modern Workplace
NSPIS	National Strategy for Police Information Systems
PKI	Public Key Infrastructure
PME	Pre-Market Engagement
POC	Proof of Concept
PP	Policies and Processes
RFP	Request for Proposal
SOBC	Strategic Outline Business Case
SOC	Security Operations Centre
UAT	User Acceptance Testing

VDR	Virtual Data Room
WMS	Witness Management System is another user interface as it shares the same platform as CMS. Its user base is the 43 Police forces of England and Wales and provides information relevant to supporting witnesses.

11. REFERENCE DOCUMENTS FROM CGI

[redacted]

Part B – Supplier Solution

1. INTRODUCTION

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

The Supplier shall provide the Services without any disruption to the Buyer and its End Users, save as otherwise set out in the Contract.

The Supplier shall supply the Services to meet the Service Requirements.

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

2. SUPPLIER SOLUTION

See the Supplier Solution attached.