CPS PRINT SERVICES

CALL OFF SCHEDULE 2: REQUIREMENTS

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

PART A: CUSTOMER REQUIREMENTS

Part A of this Call Off Schedule 2 contains the Customer Requirements and Part B of this Call Off Schedule 2 contains the Supplier Solution.

1 CUSTOMER REQUIREMENTS

1.1 Introduction

The Customer Requirements under this Call Off Schedule 2 are made up of three categories as follows:

1.1.1 Category 1 – General Requirements;

1.1.2 Category 2 – Technical Requirements, which include:-

a. Functional Requirements – services from Devices (MFDs and desktops), and Bulk Printing and Scanning services (On Premises and / Off-Site services resourced by the Supplier.)

b. Non-Functional Requirements;

c. Security Requirements; and

1.1.3 Category 3 – the Customer's Multi-Supplier Operational Environment Requirements.

1.2 Scope of the Services

1.2.1 Unless different Operational Services Commencement Dates are expressly identified in the Implementation Plan for any applicable parts of the Services, commencing on the Call Off Commencement Date the Supplier shall fulfil the following services, functions, responsibilities, requirements and deliverables (as the same may evolve during the Call Off Contract Period including adding, removing, supplementing, enhancing, modifying and/or replacing any services and/or activities or deliverables in accordance with this Call Off Contract or as otherwise Approved by the Customer in accordance with the Change Control Procedure in Call Off Schedule 12 (Change Control Procedure), from time to time):

1.2.2 the services, functions, responsibilities, requirements and deliverables that the Supplier is required to carry out as specified in this Call Off Schedule 2 and the relevant Call Off Schedules and appendices of the Call Off Contract;

1.2.3 any incidental services, functions, responsibilities, requirements and deliverables not specified in the Call Off Contract as within the scope of Supplier's responsibilities but that are reasonably and necessarily required for, or related to, the proper and timely performance and provision of the services, functions, responsibilities, requirements and/or deliverables set out in paragraph 1.2.2 of this Call Off Schedule 2; any services, functions, requirements, responsibilities and/or deliverables agreed pursuant to Call Off Schedule 12 (Change Control Procedure); and

1.2.4 subject to paragraph 1.2.5 of this Call Off Schedule 2, the services, functions, responsibilities, requirements and deliverables that the Supplier shall carry out as specified in Part B (Supplier Solution) of this Call Off Schedule 2, Call Off Schedule 4 (Implementation Plan, Customer responsibilities, Key Personnel and Sub-Contractors); Call off Schedule 5 (Testing); Call Off Schedule 6 (Service Levels, Service Credits and Performance Monitoring); Call Off Schedule 7 (Security); Call Off Schedule 8 (Business Continuity and Disaster Recovery); and Call Off Schedule 13 (Transparency Reports).

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

1.2.5 If there is any conflict between the scope of the services, functions, responsibilities, requirements and deliverables under: (i) paragraphs 1.2.2 and 1.2.3; and (ii) paragraph 1.2.4, the provisions of paragraphs 1.2.2 and 1.2.3 of this Call Off Schedule 2 shall apply and prevail.

1.2.6 The Supplier shall meet and fulfil all of the Customer Requirements in Part A of this Call Off Schedule 2 (and the Supplier confirms that the Supplier Solution set out in Part B of this Call Off Schedule meets and fulfils all of the Customer Requirements in Part A of this Call Off Schedule), as the same may evolve during the Call Off Contract Period and as they may be supplemented, enhanced, modified or replaced in accordance with this Call Off Contract, but excluding any services, responsibilities or functions that are expressly identified in the Order Form as the Customer's responsibility or a third party's responsibility.

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

2 BACKGROUND

2.1 Overview of the Crown Prosecution Service

2.1.1 The Crown Prosecution Service (the "Customer") ("CPS") is the principal prosecuting authority for England and Wales, acting independently in criminal Cases investigated by the Police and other investigators including Her Majesty's Revenue & Customs and the Department of Work and Pensions.

2.1.2 The CPS is headed by the Director of Public Prosecutions (DPP) and is one of the Law Officers' Departments. The CPS is superintended by the Attorney General who is accountable to Parliament for the Service. The Chief Executive of the CPS is responsible for the day to day running of CPS business.

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

- Advises and assists the Police during the early stages of investigations;
- Decides on the appropriate charge, in all but minor cases;
- Keeps all cases under continuous review and decides which cases should be prosecuted;
- Prepares cases for court and will either conduct advocacy in court, using an in-house lawyer resource, or instruct a self-employed advocate, generally from the criminal bar; and
- Provides information and assistance to victims and prosecution witnesses.

2.1.4 The CPS is at the core of the Criminal Justice System whereby police and other investigators address allegations and incidents and work with CPS staff to determine appropriate charges; the prosecution is prepared and presented in the Courts by CPS teams who also support victims and witnesses; and, at the close of proceedings, convicted persons are passed into the custody of Prisons and Offender Management agencies.

2.1.5 The CPS comprises fourteen (14) geographical business areas across England and Wales which administer smaller Operational Units, and CPS Direct (CPSD) which provides a twenty four (24) hour service of advice on prosecution charges to the police and other investigators. There are also three (3) central Casework divisions that handle the most serious, complex or sensitive prosecutions covering specialist

fraud, proceeds of crime, special crime and counter terrorism and organised crime. Finally, the CPS has headquarters, corporate service and operations management business functions.

2.1.6 As at January 2021, the CPS employed approximately 7,000 people, including some 2,200 Crown prosecutors and 3,600 paralegals/Case administrators, and headquarters staff. The CPS prosecutes approximately 500,000 Cases each year in magistrates' courts and about 100,000 Cases in the Crown Court. In addition to its staff working on Customer Premises, the Customer's technology infrastructure supports some 100 Police officers working from Police stations and Customer Premises and Customer staff in CPS Direct that work from courts, home and/or the Customer's Premises.

2.1.7 The services provided under this Call Off Contract are to support the CPS, the Attorney General's Office (described in the text above) and HM Crown Prosecution Service Inspectorate (HMCPSI), which inspects the work carried out by the CPS and some other prosecuting agencies.

(Clarification: The Crown Prosecution Service operates as an independent UK Government department and is **not** part of the Ministry of Justice. This means that, whilst its services may be delivered at many of the same locations as, for example, HM Courts and Tribunals Service (which is part of MoJ), it does not share connectivity and may not 'piggy-back' on existing service contracts: Customer Data on CPS systems is separately maintained and operates under different contract terms.)

2.2 Customer ICT Environment

2.2.1 The number of End Users should be estimated as around 7,000 for the Call Off Contract Period unless otherwise stated by the Customer. The Customer has approximately 50 Premises connected to two Other Supplier Data Centres via a Customer WAN

The key suppliers of services within the Customer ICT Environment are:

- Service Desk supplier
- Applications and Hosting supplier
- End User Compute supplier
- Network Services supplier

- Digital Solutions Team (internal)
- Print Services supplier
- Telephony supplier
- Mobile Telephony supplier

2.3 Current Print Services

2.3.1 The CPS' present contract for Print Services is a Call Off from Crown Commercial Service framework agreement RM 1599. CPS is now seeking to tender for new services when the current contract expires on 30 November 2020.

2.3.2 In order to allow sufficient time for the Implementation from the existing contract to new arrangements, the CPS expects to award a contract under RM3781 – Multifunctional Devices (MFDs), Managed Print and Content Services and Records Information Management.

2.3.3 CPS are seeking a three year contract with options for renewal of a total of up to a further twenty four (24) months, consisting of two (2) or more extensions, each of which can be no longer than twelve (12) months.

2.3.4 Since letting the previous contract in September 2015 the Customer's print requirement reduced significantly: court buildings were networked and cases presented digitally, a scanning backlog was addressed, and estate rationalisation by the CPS and the court service has completed and stabilised.

2.3.5 Looking to the future, some changes to the Customer's Premises may occur on a 'like for like contract' basis during the period of the next contract and digitalisation of the courts processes is expected to complete in three to four years which will impact on future print volumes.

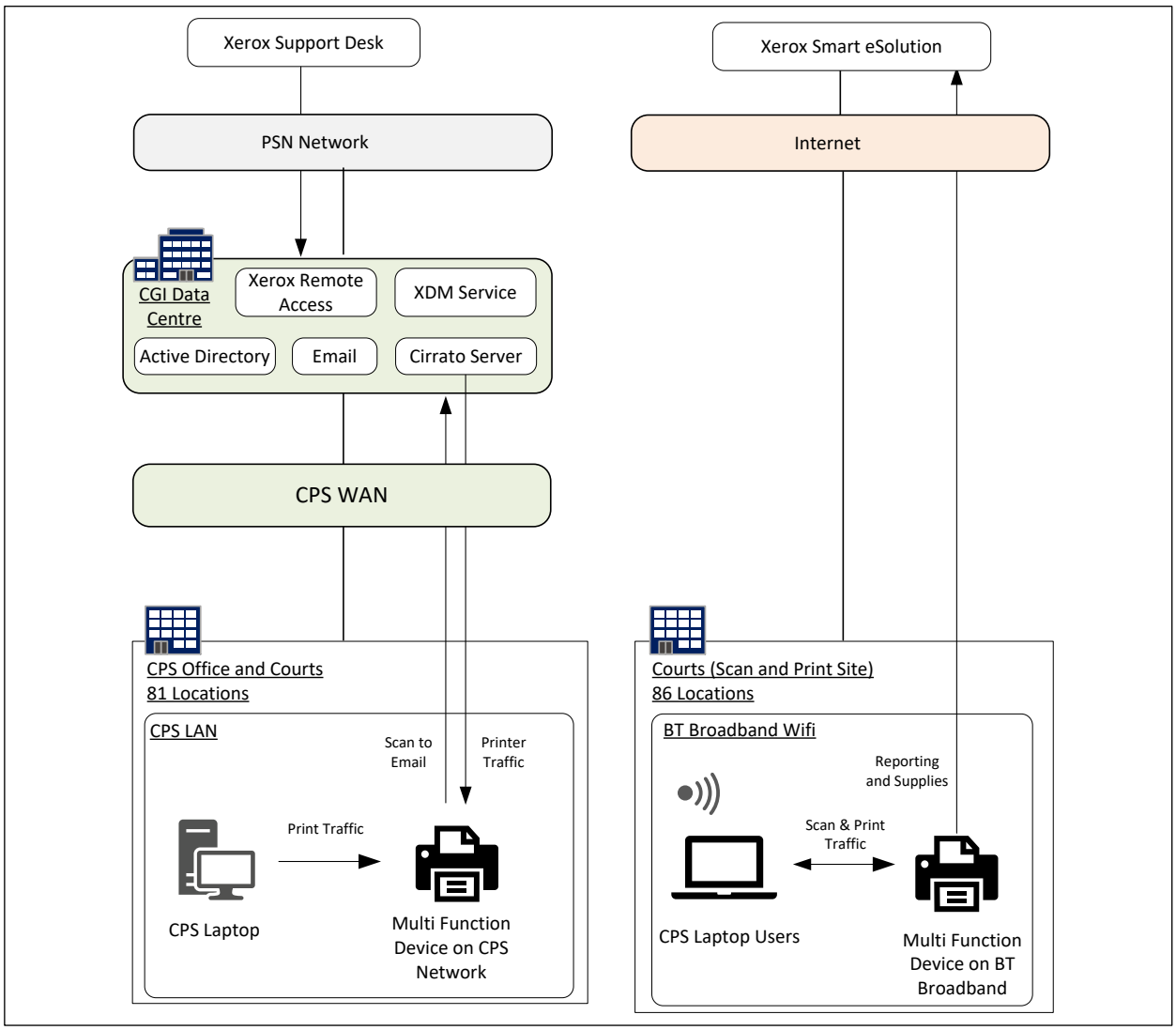
The current services consist:

- Multi-Functional Devices (MFDs). The Customer has MFDs at all Customer Premises and at Crown and Magistrates courts delivering print, copy and scan-to-email services. At the larger offices there are multiple MFDs on each floor.
- Desktop printer/scanner Devices. Devices are provided across the estate principally at non-CPS Sites, and for CPSD homeworkers. A number of devices

were retained on CPS Premises to meet local copying needs but the overall decline in print has meant that many are under-utilised.

- On Premises Bulk Printing and Scanning. The Print Service supplier provides staffed Bulk Printing and Scanning services at ten (10) of the Customer's larger Premises: On Premise and Off-Site facilities are fitted with MFDs capable of printing and scanning high volumes, and Print Supplier staff provide associated services such as flagging, binding, special copying and the creation of trial packs and Jury Bundles.
- Off-Site Bulk Printing and Scanning. The Print Service supplier has capability to collect documents for high volume copying and scanning at their secure premises.

2.3.6 The following diagram sets out the Customer's print infrastructure at a high level.



2.3.7 The current CPS print solution delivered by the Print Services supplier provides a fully managed service. The infrastructure for the solution is provided by the Apps & Hosting service supplier and is hosted in the Ark datacentres with remote access provided to Print Service End Users. The solution is based on the following components that are hosted by the Apps & Hosting service supplier:

a. Follow Print functionality – this is provided by the Incumbent's Cirrato software which removed the requirement for printer specific print queues and print servers on the CPS estate.
b. Fleet Management – the Print Service supplier's Device Manager (DM) collects information from MFDs and printers across the CPS estate and forwards the information to the Print Service supplier's Service Management Solution

2.3.8 The current Follow Print solution works well in the CPS Premises that are connected to the WAN and the Devices are located on the same network as the laptop computers. There are no print servers on the estate and the print traffic is sent directly to the Devices using the Cirrato Follow Print solution.

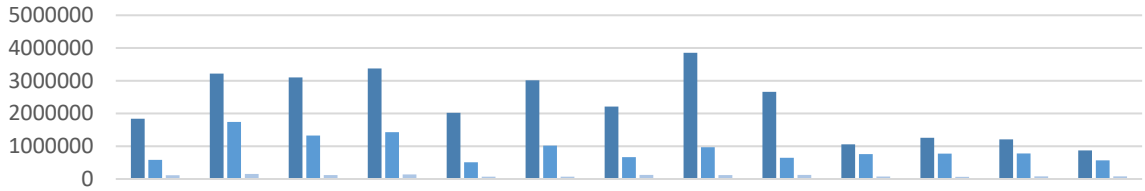
2.3.9 The business has specific difficulties printing at some court Sites where only internet connected or Zero Trust Environments are available.

2.3.10 A CPS advocate, or legal staff working for the CPS, may be required to produce on demand a scanned copy or print of new material. However, this cannot be 'ordered' by the CPS on their own laptops via court–provided connectivity services e.g. court Wi-Fi solutions. Instead the lawyer needs to retire to the CPS room in the court building where local devices are connected to BT broadband links in order to connect to the separate CPS Wi-Fi to submit jobs directly to Devices.

2.4 Print Volumes

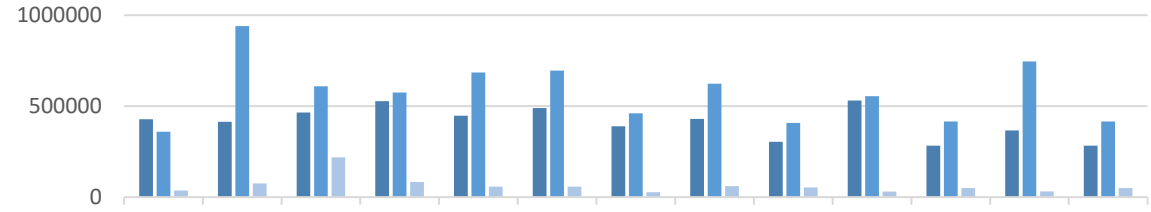
The total annual volumes of mono / colour printing, and scanning at December 2019 is shown in the figure below.

MFDs



	Dec-18	Jan-19	Feb-19	Mar-19	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19
Mono	1841468	3220739	3102903	3374646	2022328	3011727	2214121	3853756	2659852	1058245	1258383	1207544	874285
Colour	582558	1740802	1325039	1430176	509426	1020215	665929	971870	648425	760592	773108	780737	571384
Scanning	113049	154683	121495	141055	73087	70433	126060	121369	124958	78057	63857	81554	81196

Print Rooms



	Dec-18	Jan-19	Feb-19	Mar-19	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19
Mono	427942	414485	465148	527357	447408	489837	389550	430292	304377	531140	283204	366205	283204
Colour	359535	940119	609069	574758	685321	695813	461115	623304	408255	555169	415731	745858	415731
Scanning	36146	75691	218857	82884	57719	57719	27141	60547	53412	30678	49726	31057	49726

2.5 Operating systems and Office Applications

2.5.1 The Customer currently provides the following operating systems and productivity Applications to all End Users.

The core Applications include:

a. Windows 8.1 operating system (The Customer is moving to a Windows 10 environment during 2020/21)
b. Microsoft Office 365 ProPlus (Word, Excel, PowerPoint, Access).
c. Microsoft Outlook 2010
d. Microsoft Teams
e. Chrome Internet Explorer
f. Adobe Acrobat Reader (for viewing PDF documents)
g. VLC player (to support viewing multimedia evidential material)

2.6 File Storage

2.6.1 File storage is provided for each End User on a centralised server model.

Many aspects of the desktop configuration are controlled by Active Directory group policy to provide a consistent and secure desktop environment. End Users are therefore limited in what they can configure regarding the desktop environment. Only temporary data associated with specific Applications is stored on the hard disk of PC's in locations that are deemed to meet physical security requirements. End User data is held on laptop hard disks to permit off-line working but all laptop hard disks are subject to having an approved full disk encryption product installed to protect this data.

2.7 Customer Corporate Applications

2.7.1 The following paragraphs set out a set of corporate applications in use across the Customer's ICT Environment.

2.8 Case Management System (CMS) and Witness Management System (WMS)

2.8.1 The CMS is a national Case Tracking and Management System which provides case management for criminal cases. There are approximately 6,800 End Users of CMS.

CMS is a centralised application which is hosted by the Applications and Hosting supplier. The application employs a thin client architecture using IE11, DHTML, JavaScript and MS Office at the client end, client side, IIS, .NET and ASP.Net on the middle tier and Oracle (currently version 11g, being upgraded imminently to version 12) at the back end.

2.9 Prosecutor Application

2.9.1 In 2015 a Windows 8.1 Modern Application 'The Prosecutor App' was introduced to support prosecutors in court including recording the outcome of hearings. This touch enabled application communicates with the central CMS system using web services when online and stores information locally when offline.

2.10 Management Information System (MIS)

2.10.1 Associated with CMS/WMS is a Management Information System (MIS) that provides statistical and summary information on the progress of cases. This is based on Business Objects Web Intelligence and has around 200 End Users.

2.11 Enterprise Resource Planning (ERP)

2.11.1 The Customer uses an Oracle Cloud application to deliver central finance, procurement and HR services.

2.12 The Customer's Digital Solutions Team

2.12.1 The Customer's Digital Solutions Team have implemented the following service changes since 2019:

- Move from On Premises to Cloud Services
    - Office 365 Email
    - Office 365 One Drive for Business (ODFB)
    - Cloud based fileshares (Microsoft Azure)
    - Microsoft Teams
- Consuming Software as a Service (SaaS)
    - Service Now (Customer's ITSM tool)
    - Oracle Cloud ERP
- Volumes of Multimedia to and from Cloud Services

These developments are expected to continue with the introduction of the following in 2020/21:

- Use of Visio Based documentation for the Customer's Standard Operating procedures
- Use of Artificial Intelligence to support evidence gathering and Disclosure
- Full digitisation of case files including Video enabled justice and Digital Evidence transfer
- Windows 10
- Enhancement to ServiceNow to support all processes
- Security enhancements

2.13 Summary of the Customer's Multi-Supplier Operational Environment

2.13.1 Further to working under an earlier single source contract for IT services, the Customer has progressed its digital journey and recognises that it is dependent on a Multi-Supplier Operational Environment to deliver and maintain the IT services and consumables that are required to support the prosecution services that Parliament and the public requires of it.

2.13.2 The key suppliers of services within the Customer ICT environment (listed in paragraph 2.2.1 of this Call Off Schedule 2) are contracted to provide services to the

Customer and also to act on the instructions, and within the guidance, of the Customer's Agency Manager to provide non-operational functions that include, but are not limited to:

- maintenance of Policies, Procedures and Processes (PPPs) aligned to the Customer's policies
- response and management of Major Incidents
- Governance
- protection of the Customer Data
- collation of activity to address supplier interdependencies and Upgrades
- proactive collaboration with the Customer and Other Suppliers
- Continuous Service Improvement

2.13.3 In summer 2018 the Customer assumed the role of Agency Manager or Service Integration and Management (SIaM) for its IT Environment. The Customer's in-house teams provide the following support for the IT environment:

- Service Procurement and Commercial / Contract Management;
- High Level Architecture & Design,
- Portfolio Governance and Control (e.g., Change Management);
- Change Delivery;
- Service Design and Management (PPP's, Service Assurance, Contract Management).

2.13.4 The Customer has appointed its Service Desk supplier to support the Multi-Supplier Operational Environment in respect of:

- Incident Management,
- Problem Management,
- Event Management,
- Request Fulfilment Management,
- Access Management,
- Knowledge Management,
- Master CMDB (SACM) Management; and
- Service Reporting.

2.13.5 In addition to the services identified as SiaM responsibilities above, the following known services also form part of the Customer's ICT Environment (not an exhaustive list):

- Microsoft 365 (supported in-house);
- Oracle-based ERP;
- Video-conferencing (contracted with Vodafone);
- a variety of portal based subscription services, for example:
    - Data Transfer (hosted by Egress);
    - On-line learning & development (hosted by Lumesse);
    - Payroll (hosted by iPayView);
    - Westlaw (hosted by Thompson Reuters);

2.13.6 The Supplier is expected to actively work with the Agency Manager and to contribute to achieving the best possible service for the Customer via a Continuous Service Improvement approach.

3 CATEGORY 1 – GENERAL REQUIREMENTS

#	**Requirement**
PRI/R/GREQ/01	The Supplier shall deliver all Services in accordance with the terms of the Call Off Contract, including the Standards.
PRI/R/GREQ/02	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 Customer (e.g., operating models based on COBIT (Control Objectives for Information and Related Technology), TOGAF (The Open Group Architecture Framework), and ITIL (Information Technology Infrastructure Library)).
PRI/R/GREQ/03	The Supplier shall use ITIL based processes and perform the Services in accordance with industry based best practice and, if required, the Supplier shall demonstrate this to the satisfaction of the Customer.
PRI/R/GREQ/04	The Supplier Solution shall be implemented in a modular and commoditised way, allowing for flexible and scalable Services that can be updated and replaced with minimal disruption to the Customer.
PRI/R/GREQ/05	The Supplier shall ensure that its Solution shall be designed for process integration with the services of current Other Suppliers, as well as future Other Supplier solutions.
PRI/R/GREQ/06	The Supplier shall automate the Services wherever possible to ensure that maximum process efficiency and data quality are obtained in relation to the Services. 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.
PRI/R/GREQ/07	The Supplier shall facilitate Process efficiency by choosing automation over manual intervention and empowering the business to self-serve, subject to such automation being Approved by the Customer in advance.
PRI/R/GREQ/08	The Supplier shall support all of the ITIL functions set out under the heading “Non-Functional Requirements” in this Call Off Schedule 2, and in doing so interact with the Customer’s SiaM function as set out in the Customer’s Policies.

#	**Requirement**
PRI/R/GREQ/09	The Supplier shall ensure that their Policy, Processes and Procedures for all the services under this Call Off Contract adhere to and integrate with the existing ITIL function related Customer policies and Processes, which will include (but not be limited to): • Incident Management (including Major Incident Management) • Problem Management • Service Asset and Configuration Management Database (CMDB) provision. • Change Management – Operational • Change Management – Commercial • Request Fulfilment • Release Management • Performance Reporting • Knowledge Management
PRI/R/GREQ/10	The Supplier shall ensure that Processes for all ITIL functions are aligned with the Policies set out by the Customer by the end of Implementation.
PRI/R/GREQ/11	The Supplier shall provide support to the Other 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.
PRI/R/GREQ/12	The Supplier shall ensure that, upon request from the Customer, certain of: (i) the Supplier's Representative; (ii) and any of the Key Personnel; and/or (iii) other relevant persons identified by the Customer, that the Customer wishes to meet, shall attend workshops or meetings with the Customer and/or any other supplier as the Customer deems necessary throughout the Call Off Contract Period.
PRI/R/GREQ/13	Where the Supplier fails, or becomes aware that it is likely to fail, to comply with any obligation of this Call Off Contract and such failure may impact on the performance of the Services by the Supplier (including the Service Levels), the Supplier shall, as soon as is reasonably practicable, notify the Customer of such failure or likely failure.
PRI/R/GREQ/14	The Supplier shall access and use the Customers ITSM tool (ServiceNow) for the management of Service events across the Service Management Lifecycle.

#	**Requirement**
PRI/R/GREQ/15	The Supplier shall ensure the updating of Service event data shall occur immediately, or as soon as is reasonably practical, in sufficient time to enable the production of management information that can be acted upon to maintain Service Levels, Service Level Targets, and Key Performance Indicators for the Services.
PRI/R/GREQ/16	The Supplier shall bear the cost of decommissioning, collection and disposal of the Supplier's Equipment.
PRI/R/GREQ/17	The Supplier shall wherever possible use simplified assurance and payment processes and will meet the Customer's electronic invoicing requirements when invoicing the Customer. (Clarification: The Customer's preference is that the Supplier submits valid, electronic invoices to its billing system. Invoices can be accepted in scanned form.)
PRI/R/GREQ/18	The Supplier shall use the Customer's ITSM tool ServiceNow to raise and progress Invoices.
PRI/R/GREQ/19	The Supplier shall adhere to its obligations to ensure the timely payment of its Supply Chain – as set out under Procurement Policy Note 04/19 (Suppliers' approach to Payment).
PRI/R/GREQ/20	The Supplier shall ensure that all necessary support is provided to the Customer, or any Auditor assigned or appointed by the Customer, to audit any aspect of the Services provided by the Supplier.
PRI/R/GREQ/21	The Supplier shall comply with Data Protection Legislation and data protection provisions set out in the Call Off Contract, including Clause 34.7 and relevant Call Off Schedule 17 (Data Processing), and including in relation to the processing of the Personal Data controlled by the Customer.
PRI/R/GREQ/22	The Supplier shall retain Customer Data as necessary beyond the expiry or termination of the Call Off Contract where it is required to do so under the provisions of Clause 34.7 and Call Off Schedule 17 (Data Processing).
PRI/R/GREQ/23	The Supplier shall acknowledge that the Services shall be delivered in a manner which is compliant with the Customer's Welsh language scheme and where required any change required to ensure such compliance shall be subject to the Change Control Procedure. The Supplier shall ensure that it is familiar with the Customer's current Welsh language scheme which is available within the VDR.

#	**Requirement**
	(Clarification: The Customer operates in both England & Wales and, whilst none of the Call Off Contract Services will be delivered to members of the public, the Welsh Language provisions could apply. Notwithstanding Changes in Law that might affect the future, the contract position is that no 'Print Service' documentation is required to be delivered in the Welsh Language and the implementation of any operational changes will be handled through the Change Control Procedure.)
PRI/R/GREQ/24	The Supplier Solution shall adopt a Continuous Service Improvement approach that meets the Supplier's Framework-level obligations to the Crown Commercial Services and, under this Call Off Contract, supports the Customer and Other Suppliers by: • optimising the effectiveness and efficiency of the Customer's IT service management processes; • supporting collaborative working and the improvement of Service outcomes; and • Informing the Customer of technical innovation that may contribute to the development of the Services.
PRI/R/GREQ/25	The Supplier shall replace all print devices that are no longer supported (End of Life) at no cost to the CPS. This includes print devices that may have been ordered via the Customer's Service Catalogue

4 CATEGORY 2 – TECHNICAL REQUIREMENTS

4.1 Summary of technical requirements

In respect of the future requirement the following section documents the requirements including the technical requirements for the MFD Devices and Bulk Printing & Scanning.

Key outcomes for this contract

- High quality print services, both in respect of reliable devices, and functionality of the devices meet the needs of everyone in CPS
- Ensure CPS people have the right tools and skills to deliver the highest quality service with the right technology
- Consistency of services available across CPS, aligned to business need
- Clear monitoring to enable proactive maintenance and continuous service improvement,
- Service that is easy to support and flexible

Key scenarios / needs:

- Efficient and secure methods for Bulk Printing and Scanning – most notably jury bundles – including the courier delivery to the required location where completed offsite
- High quality guarantee for photographs / key evidence
- Colour and B&W Printers available at CPS locations based on business need / demand
- Colour printers in Crown Courts to allow the printing of last minute changes to jury bundles
- Appropriate use of scanning [to email] technology to support business processes
- Desktop printers by exception for ITA users / special circumstances

Key expectations on the manner of delivery of the contract

- Increase business efficiency to support our goal of digitising the Criminal Justice System.
- Deliver a low risk Implementation ensuring continuity of service whilst maintaining the highest level of End User experience throughout the Implementation period
- Support the print service with experienced Supplier Personnel managing and delivering the contract with innovation, and Continuous Service improvement

Scope: The scope of the re-tender includes the following broad requirements, described in further detail below in summary level and in more detail within technical requirements sections, which follow:

- Provision of an appropriate number centrally managed Multi-function Devices (MFD) providing photocopy, scanning and print capability: this to include some small form factor Devices that can be housed on a desktop.
- Provision of a Bulk Printing and Scanning services (hosted at on-Premises or off-Site facilities depending on Supplier proposals) including the option to have documents delivered to CPS Sites.
- Ability for the End Users to print in Courts

Multi-functional devices:
Approximately two thirds of printing, scanning and copying is carried out within the Customers Premises, used to prepare cases.

The Solution must meet the Security requirements (see section 5 below) and must also provide a straightforward easy-to-use solution for End Users that is reliable. For example, the current solution of 'Follow Print' is well established and supports ease-of-use and security.
A proportion of MFD use is carried out in the Crown and Magistrates courts; the courts are not Customer Premises and the Customer is seeking a comprehensive solution, to support prosecutors and Legal support staff who need to print some documents in courts. The Customer's initial preference would be to move to a solution, particularly for printing in court, but this could also be use in standard offices, where print jobs are sent to a cloud based location, stored securely and can then be printed in court subject to the End User confirming their identity as the originator of the print request.

There is a requirement to provide colour printers of a suitable quality to print some documents in high resolution colour specifically at Crown Courts, where colour photographs make up a proportion of the papers required for the jury. The current MFDs in Crown Courts are monochrome only.

Document print and scan quality is paramount and is required to be maintained throughout the lifecycle of each Device.

Small form factor printers or desktop printers are required for the following situations:

- CPSD Home workers – approximately 140 prosecutors work from home to provide a 24hr service; some 40 of these End Users require a printer capable of printing case papers due to ITA (see below).
- IT Accessibility (ITA) End Users – this group of users including, but not limited to CPSD staff, have a reasonable adjustment requirement for desktop printers

General operation of MFD fleet; a key aspect is the proactive monitoring and preventative maintenance approach to ensure all Devices are operating

Future requirements
Looking to the future, some changes to the Customer's Premises may occur on a 'like for like contract' basis during the period of the next contract and digitalisation of the courts processes are expected to result in for example, the digitisation of information for the jury.

Printing services
The printing solution should be flexible enough to cater for all the CPS connectivity requirements and provide the End Users with an easy to use, secure and fully functional print service wherever they are located.

There are two main connectivity scenarios across the CPS estate that the Supplier Solution shall be able to accommodate, these are:

Scenario 1 – Printing in Crown Courts and HQ Sites
The printer is installed on CPS Local Area Network (LAN) and the End User could be connected directly to the Customer System within the building or by using the Wi-Fi solution within the building to Virtual Private Network (VPN) back to the Customer System. The process of printing should be identical whether they are connected to the System or to the Wi-Fi.

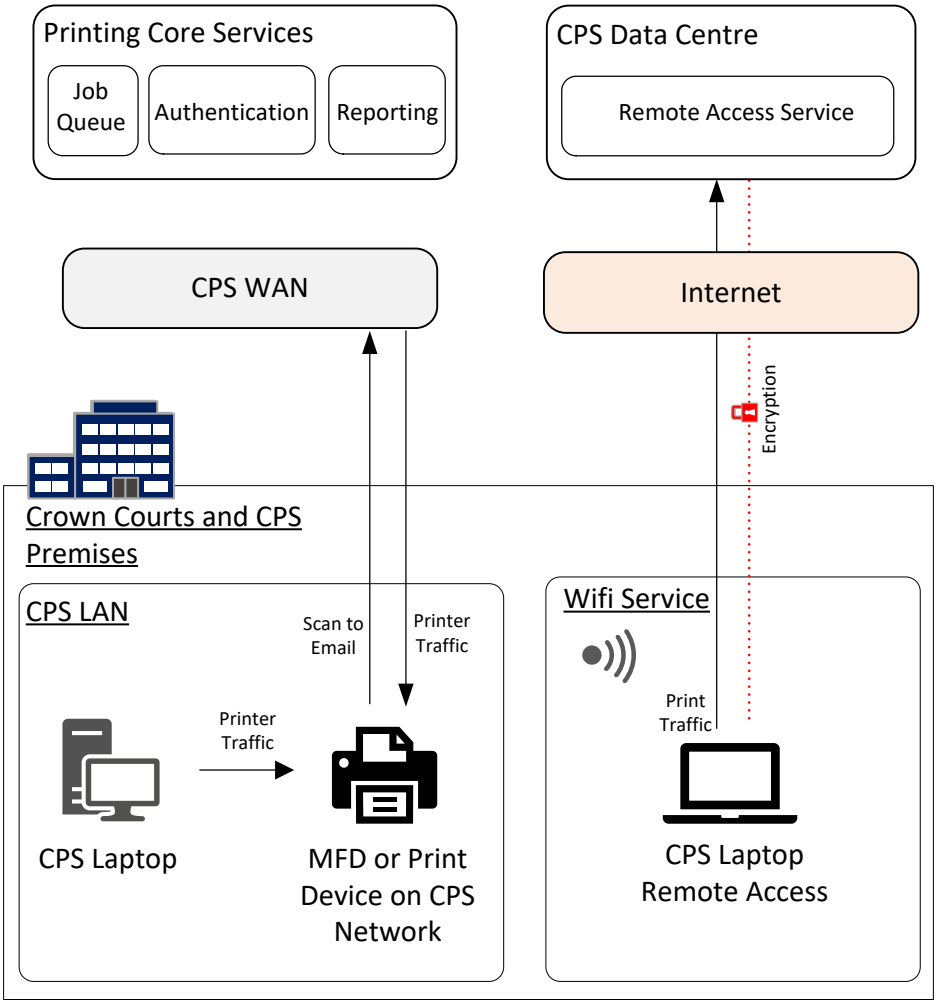


Figure 1 – Printing service - Scenario 1

Key service points:

a. CPS laptop printing uses a key fob or Radio Frequency Identification (RFID) tag to identify the user, once identified the print job is submitted directly to the MFD or the print Device by the desktop machine.
b. CPS End User could be connected across the internet using a VPN and the print traffic will have to travel across the VPN to the Customer System. The authentication and pull print functionality are the same as printing from the desktop machine.
c. The Solution should enable seamless printing but also scanning of documents to CPS email from MFD Devices.
d. The majority of End Users will be using a laptop device on the Customer System and will print to their local Multi Functional Device.

Scenario 2 – Printing in Courts and Zero Trust Environments

This printing use case is seen in Magistrates courts and Zero Trust Environments with no access to the Customer System and the only connectivity is using an internet connection on the site. Within Magistrate courts there is existing PCU Court Wi-Fi connectivity to the internet and at government hub buildings that have internet access throughout the building using Gov-Wi-Fi and direct connectivity.

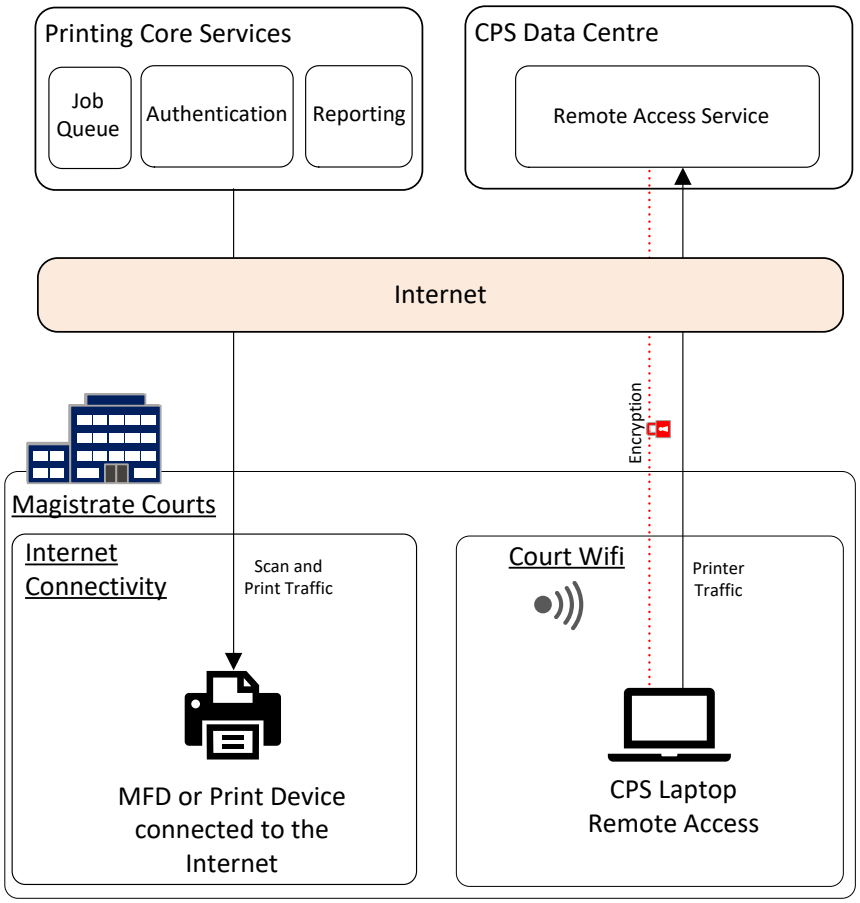


Figure 2 – Printing service – Scenario 2

Key Service Points

a. The CPS laptop will be connected to the internet using a VPN connection across the internet. The MFD device will also be connected to the internet but this might not be the same internet solution within the site.
b. The laptop user should be able to securely print to the MFD on an internet only connected site or zero trust environment.
c. The authentication and pull print functionality should be consistent across all the connectivity scenarios.

Bulk printing and scanning services.

The Customer is looking for an approach to Bulk printing and scanning services which fully supports their current working practices, in that large documents or large sets of documents are produced and delivered to the appropriate place, either to the Customer's offices or direct to the courts, via the Supplier delivery service.

The Customer is familiar with the use of couriers to deliver between office and courts, and it looking to a reliable, fast and efficient Supplier delivery service to be provided to meet the demands of court hearing deadlines.

The detail of the current volumes and nature of Bulk printing and scanning services is provided in the VDR. Example documents and documents sets including the details of the collation and presentation standards are provided.

4.2 **Functional requirements**

4.2.1 **Generic Printing & Scanning**

#	Requirement
PRI/R/GPRINT/01	The Supplier Solution shall provide a full maintenance service for each Device, including preventative maintenance, the provision of print Consumables, spares and or replacement devices where required.
PRI/R/GPRINT/02	The Supplier Solution shall provide a fast, reliable and secure printing service to all the Customer Sites.
PRI/R/GPRINT/03	The Supplier Solution shall provide a scalable and flexible architecture that can support the business capacity demands over the term of the Call Off Contract.
PRI/R/GPRINT/04	The Supplier Solution shall ensure sufficient Devices are deployed to ensure a resilient service to the End Users at each of the Customer's sites.
PRI/R/GPRINT/05	The Supplier Solution shall provide reliable and energy efficient Devices that can manage the 'normal' print demand for each specific Site. The Supplier shall demonstrate appropriate resilience to ensure that the continuity of Services is not disrupted by Device breakdowns.
PRI/R/GPRINT/06	The Supplier Solution shall accommodate normal business demand in line with current volumes within a reasonable volume tolerance in order that the Supplier successfully manages both the risks of damage to Devices from running over-capacity and poor value by running consistently under-capacity.
PRI/R/GPRINT/07	The Supplier Solution shall ensure flexible and responsive services to replace individual Devices – preferably within existing stocks – to upgrade or downgrade Devices that demonstrate a pattern of running over or under capacity, or to replace Devices that demonstrate a pattern of breakdowns and maintenance problems.

#	Requirement
PRI/R/GPRINT/08	The Supplier Solution shall moderate the number of Device models in use across the estate to simplify maintenance and support the resilience of Services.
PRI/R/GPRINT/09	The Supplier Solution shall enable the use of Government Buying Standard (GBS) paper products without detriment to the Services. The Customer will continue to be responsible for the purchase of paper products. (GBS paper products meet the majority of all print needs. However, in exceptional circumstances non-GBS paper (i.e. a brighter white) is used by Customer Staff to produce illustrations for prosecutions. Although this is minimal, and print volumes may continue to decline, the products must be capable of being utilised – and this may require Supplier Personnel to work with Customer Staff to enhance print quality for limited jobs.)
PRI/R/GPRINT/10	The Supplier Solution shall enable default settings to be applied to Devices with options for End Users to over-ride for single occasions. The Customer anticipates that the majority of machines will be set to duplex (double-sided) printing and copying as the default option with the settings for Devices at pre-determined locations set for single-sided printing and copying: the pre-determined locations shall be confirmed between the Parties during Implementation.
PRI/R/GPRINT/11	The Supplier Solution shall support the Customer's End Users working from home. The Supplier shall ensure support includes printing (where the End User has access to a Desktop Device supported under this Call Off Contract)
PRI/R/GPRINT/12	The Supplier Solution shall ensure End User can print to Devices twenty four (24) hours a day, seven (7) days a week.
PRI/R/GPRINT/13	The Supplier Solution shall be delivered as Software as a Service delivery model Where other service delivery models are proposed this should be agreed by the Customer.
PRI/R/GPRINT/14	The Supplier Solution shall provide application level tenancy separation when used in a shared service. This will allow the Customer to use the solution in a multi-tenancy environment.
PRI/R/GPRINT/15	The Supplier shall, where possible deploy a single universal, device agnostic print driver that can be deployed to the Customer Devices.

#	Requirement
PRI/R/GPRINT/16	The Supplier Solution shall not rely on site-based print servers for the Solution to function.
PRI/R/GPRINT/17	The Supplier Solution shall be able to securely operate within Zero Trust Environments where there is only internet connectivity available on the site.
PRI/R/GPRINT/18	The Supplier Solution shall be able to function when an End User is connected to the Customer System using a VPN and Remote Access Service (RAS). The End User experience should be identical to when the End User is directly connected to the Customer System.
PRI/R/GPRINT/19	The Supplier shall proactively monitor the Equipment provided as part of the Supplier Solution to detect, isolate and facilitate the resolution of issues before they become Incidents.
PRI/R/GPRINT/20	The Supplier shall document, and provide the Customer with written details of the Dependencies on the Customer, Customer's SiaM and Other Suppliers including: (1) the testing and distribution of printer device drivers; (2) the testing and distribution of any other Software; (3) the availability of adequate space and power; (4) the provision of an Active Directory domain for authentication and any required changes in support of the Supplier Solution; (5) the provision of adequate WAN and LAN bandwidth; (6) training for End Users in relation to print devices; (7) cabling of the networked print device to the wall or floor port; (8) provision of print queues and print mapping to the networked print device; (9) enabling and integration of 'scan to email' with the Customer's email solution; (10) hosting of servers within the Customer's SiaM or Other Suppliers' data centre to allow for the collection of Management Information; (11) WAN connections between the Supplier, the Customer, the Customer's SiaM or any Other Suppliers'
PRI/R/GPRINT/21	The Supplier Solution (for MFDs and Bulk printing & scanning) shall ensure: a. Scanning is set to 200 Dots Per Inch DPI) as a minimum. b. Scanning quality can be modified to support up to 4800 DPI where necessary c. Both colour as well as black and white scanning is possible d. The End User is able to select JPEG, TIFF or PDF as the preferred scanned output format.

4.2.2 Printing equipment

a. MFD Devices

#	Requirement
PRI/R/DEVICE/01	The Supplier Solution shall offer MFDs with a minimum functionality as follows but not limited to: 1. print to A4 paper; 2. print to A3 paper; 3. print to A5 paper; 4. print in black and white; 5. print in colour; 6. print single and double sided; 7. collate output; staple output; 8. hole punch options 9. scan a document and send the output to any CPS email address; 10. print on labels; 11. re-paginating a document as its various component parts are being copied and printing out copies with the new page numbers
PRI/R/DEVICE/02	The Supplier Solution shall ensure an End User's print request is held until the End User: a. presents an individually defined key or RFID (Radio Frequency Identification) tag at the print device, b. authenticates and releases, c. cancels the request, or d. 24 hours have elapsed since the submission of the print request at which point the request will be automatically deleted. e.
PRI/R/DEVICE/03	The Supplier shall: a. Provide individual keys or RFID tags for all of the Customer's End Users during the Implementation Period b. Make additional individual keys or RFID tags available via the Customer's Service Catalogue c. Replace damaged or non-functioning individual keys or RFID tags.
PRI/R/DEVICE/04	The Supplier Solution shall provide the Customer with electronic copies of user manuals for every MFD printer model that is a part of the Solution. Additionally, the Supplier shall provide and maintain close to each Device: a. a quick reference guide to key functionality for each Device; and b. a note of Model Number/Asset descriptor that End Users can reference when requesting Service Desk/Supplier assistance.

b. Desktop Devices

#	Requirement
PRI/R/DESK/01	The Supplier Solution shall offer desktop Devices with a minimum functionality as follows: a. print to A4 paper; b. print in black and white; c. print in colour; d. print single and double sided; e. collate; f. scan a document and send the output to a CPS email address.

4.2.3 Device Management

#	Requirement
PRI/R/DEVMGT/01	The Supplier Solution shall provide for the maintenance and support of: (a) Networked Devices (including MFDs); and (b) Non-Networked Desktop Devices (approved by the Customer's Service Delivery team)
PRI/R/DEVMGT/02	The Supplier shall provide, manage, support and decommission Devices in accordance with the Service Levels set out in Call Off Schedule 6 (Service Levels, Service Credits and Performance Monitoring) and in accordance with Schedule 7 (Security).
PRI/R/DEVMGT/03	The Supplier shall provide, install, maintain and decommission all Devices identified as part of the Supplier Solution in accordance with all relevant print device manufacturer support dates.
PRI/R/DEVMGT/04	The Supplier shall bear the cost of decommissioning, collection and disposal of any redundant Equipment, including on expiry or termination of the Contract (or part thereof, as applicable) that is: (i) a part of the Supplier Solution; or (ii) which relates to any Equipment taken on by the Supplier during Implementation.
PRI/R/DEVMGT/05	The Supplier Solution shall demonstrate proactive MFD fleet maintenance on Devices at the Customer's Premises with the aim of optimising the performance of the MFD fleet and reducing the number of Device-related incidents.
PRI/R/DEVMGT/06	The Supplier shall provide an Install, Move, Add, Change and Dispose (IMACD) process to ensure that all Devices under this Call Off Contract remain fully supported throughout the Device lifecycle.
PRI/R/DEVMGT/07	The Supplier shall: a. Work with designated individuals at each of Customer Premises to ensure successful delivery of Consumables to Customer Sites. Designated individuals or roles shall be agreed during Implementation.

#	Requirement
	b. Ensure that all devices that are a part of the Supplier Solution shall be able to anticipate consumable depletion (with the exception of legacy desktop printers as appropriate) and report this to the Supplier such that Consumables are dispatched to the relevant Customer Sites under Just In Time principles.
PRI/R/DEVMGT/08	The Supplier shall, at the request of the Customer, arrange for the removal of surplus Consumables (generated by flaws in the Supplier's automated stock ordering system?) from Customer Sites, and demonstrate their economic re-use on the Customer's estate.
PRI/R/DEVMGT/09	The Supplier Solution shall include: a. Processes to swap out or remove a defective or under-performing Device, and to act at the Customer's request to implement such a change. b. Agreeing the reason for Device replacement; c. Confirming the functionality of the new Device. d. Removal and disposal of Devices, Consumables and other equipment provided by the Supplier from the Customer's Sites in accordance with statutory requirements.
PRI/R/DEVMGT/10	Where a Device is not connected to the Customer's LAN, the Supplier Solution shall still ensure Management Information is collected from the Device in respect of each Service Measurement Period and included within the overall Performance Monitoring information provided for the Services.
PRI/R/DEVMGT/11	The Supplier shall supply the Customer with Performance Monitoring Information in respect of each Service Measurement Period, including but not limited to: a. number of impressions printed; b. number of black and white impressions printed; c. number of colour impressions printed; d. number of scanned images captured? e. number of paper jams; f. number of toner low alerts; g. number and type of high volume print jobs undertaken; h. utilisation statistics for each Device; and i. equipment availability statistics for each Device. volume of print impressions and scanned images capture at the Supplier's off-Site facilities
PRI/R/DEVMGT/12	The Supplier shall provide a Systems Measurement Document that sets out the calculation for each Service Level set out in Call Off Schedule 6 (Service Levels, Service Credits and Performance Monitoring) of this Call Off Contract and the people, Process and technology used to collate the data that is required for such calculations. The Systems Measurement Document shall be agreed with the Customer's SIaM and the Customer prior to the first Operational Services Commencement Date.

#	Requirement
PRI/R/DEVMGT/13	The Supplier Solution shall proactively monitor the Devices to detect, isolate and facilitate the resolution of problems, events and Customer issues before they become Incidents.
PRI/R/DEVMGT/14	The Supplier shall provide a logging and notification system to the Customer which details issues regarding the functional status of Devices. These details shall include but not limited to: a. misfeeds; b. paper jams; c. alerts for low Consumables / insufficient toner; d. variable print density across a page; and e. Device faults that may result in a loss of functionality. Further, the Supplier shall aim to resolve functional matters in order that Service Levels are met.
PRI/R/DEVMGT/15	Within five (5) Working Days (or such other period as the Parties may agree in writing) of the end of each Service Measurement Period, the Supplier shall provide a Performance Monitoring Report to the Customer.
PRI/R/DEVMGT/16	The Supplier Solution shall provide accurate and timely Management Information to the Customer's SIaM and the Customer.
PRI/R/DEVMGT/17	The Supplier Solution shall provide the number of scan to email requests by device, satisfied within the Service Measurement Period.
PRI/R/DEVMGT/18	The Supplier Solution shall provide the average speed to copy/print for each Device.

4.2.4 **Print Quality Management**

#	Requirement
PRI/R/PRIQUAL/01	The Supplier Solution shall ensure the quality of printing is maintained by: a. Ensuring all print devices provided are capable of automatic calibration; b. Ensuring such calibration occurs at least once a month; c. Ensuring the output from such calibration is collated and statistics of failed and passed calibrations along with narrative is provided in the performance monitoring report; d. Ensuring any issues highlighted by the automatic calibration are resolved before they are reported as Incidents. e. Providing management information (including where appropriate the replacement of print devices) to the Customer on a monthly basis; f. Resolving Incidents raised due to poor quality printing; g. Ensuring the number of Incidents raised due to poor quality printing is reported under a “Quality” heading in the performance monitoring report.
PRI/R/PRIQUAL/02	The Supplier Solution shall ensure that: (1) There is a clear definition of when a page is classified as colour (2) page should be counted as either colour or monochrome (3) A pure monochrome page shall be counted as monochrome; and (4) pages printed as grey scale shall be counted as monochrome.
PRI/R/PRIQUAL/03	The Supplier shall classify repeat Incidents related to the same print device as a Severity Level 2 Incident (where such repeat Incidents have not already been classified at a higher Severity Level).
PRI/R/PRIQUAL/04	The Supplier Solution shall capture, store and allow Supplier Personnel adequate access to Site details required for the installation, maintenance and decommissioning of print Devices. (e.g. parking facilities, stairs to be negotiated, small doorways, site opening hours, site primary and secondary contacts, etc.)

4.2.5 **Bulk Printing and Scanning**

#	**Requirement**
PRI/R/BULK/01	The Supplier Solution shall offer Bulk Printing and Scanning services from the Supplier facilities ('Off-Site') or the Customer's Premises ('On-Premises') as agreed by the Parties.
PRI/R/BULK/02	The Supplier Solution for Bulk Printing and Scanning services shall be available: For Example, (a) at facilities on the Customer's Premises ("On-Premises") Mon – Fri 07:00 to 19:00 on any Working Day; (b) at secure facilities provided by the Supplier on their own property ("Off-Site") with the capability to accept orders for print by email 24/7 Clarification: this Part A Requirement reflects the Customer's general requirement with the contracted agreement set out in the corresponding response in Part B.
PRI/R/BULK/03	The Supplier shall ensure that sufficient Supplier Personnel are available at each Bulk service facility during the Working Day to ensure that print Requisitions are able to be accepted by Supplier, and the Supplier shall provide trained staff to provide, and advise the Customer's Staff on, the Bulk services including the options for enhancing the quality of copy, where poor quality original documents are received from the Customer.
PRI/R/BULK/04	Where the volume of printing or copying requested by the End User is unusually high, the Supplier may fulfil the requirement via other off-site print capability, but only with the Customer's prior agreement.
PRI/R/BULK/05	The Supplier Solution shall provide minimum Bulk printing and scanning functionality and finishing as follows but not limited to: a. able to print to A4 paper; b. able to print to A3 paper; c. able to print to A5; d. able to print in black and white; e. able to print in colour; f. able to print single and double sided; g. able to collate output; h. staple output; i. hole punching; j. comb binding; k. wire binding; l. stapled metal clips; m. heat binding; n. scanning to email; o. disc burning; and

#	**Requirement**
	p. saving scanned output to CD, DCD or encrypted memory stick. q. printing on labels; r. re-paginating a document as its various component parts are being copied and printing out copies with the new page numbers; and s. laminating The Supplier Solution shall ensure the ability to produce material in non-standard formats as directed by the Customer.
PRI/R/BULK/06	The Supplier Solution shall be capable of scanning hard copy, printing the scanned file as per the Requisition and saving the scanned file to a shared area to be agreed with the Customer during Implementation.
PRI/R/BULK/07	The Supplier Solution shall allow for optical character recognition on all scanned documents.
PRI/R/BULK/08	The Supplier Solution shall allow for paper archives to be digitised (scanned and saved to a shared drive or CD).
PRI/R/BULK/09	The Supplier shall accept orders for Bulk services from the Customer's End Users by the completion of an online or hard copy Bulk services Requisition. Typically this will include: The Supplier shall ensure each print requisition submitted by an End User shall include, as a minimum, the following information: (1) number of copies required; (2) number of pages; (3) date and time ordered by End User; (4) turn around time requested; (5) End User contact name, department, telephone number and email; (7) size of paper; (8) duplex or single sided; (9) approved cost centre codes; and (10) whether colour printing is required; (11) details of any additional finishing requirements;
PRI/R/BULK/10	The Supplier shall ensure that the Customer is contacted in the event the Supplier receives multiple print requests of conflicting priority, such that the Customer may determine the relative degree of urgency and provide instructions to the Supplier accordingly.
PRI/R/BULK/11	The Supplier shall, upon request by the Customer, arrange delivery of copy to any of the Customer Sites. In the event the Supplier arranges delivery at the Customer's request, the Supplier shall use their own delivery service

#	**Requirement**
PRI/R/BULK/12	In the event the Supplier arranges collection or delivery services at the Customer's request, the charge for carriage will be added to the Customer's next invoice.
PRI/R/BULK/13	The Supplier shall ensure that [On Premise and Off-Site] facility Devices shall be able to direct scanned output to a CPS email address nominated by an End User.
PRI/R/BULK/14	The supplier shall ensure the adherence to bulk print delivery timescales at all times, and maintain their own contingency plans to overcome resource shortfalls.

4.2.6 **Specialist scanning request service**

The Customer's Management Information Unit and Appeals divisions require bespoke scanning services to address Subject Access Requests and preparation for Appeal hearings under which CPS case officers may need to assemble mixed media of variable quality and high sensitivity dating back up to 30 years for conversion to a catalogued, digital format.

- Request material may then need to be processed by End Users before release to an individual under strict statutory timescales. Under existing arrangements, this work is dealt with on-Premises as a high priority; and
- Appeals and VRR casework has scope to go further back than 30 years on rare occasions, with a recent case requiring review requiring access to case material from late 1970s. This affects the physical condition of the material and requires manual handling during scanning with frequent checks & action to ensure optimal quality of the scanned outputs. Under existing arrangements, the work is handled on-Premises to carefully managed timescales.

#	**Requirement**
PRI/R/SPECIAL/01	The Supplier Solution shall ensure that original hard copy is returned to Customer in the same condition as received i.e. there may be a need to remove staples, post-its etc. before scanning, anything removed would be replaced and the contents returned to the boxes tied in bundles as found.
PRI/R/SPECIAL/02	The Supplier shall on request, ensure priority scanned output is made available within three (3) Working Days. This will require Supplier Personnel to prioritise jobs.
PRI/R/SPECIAL/03	The Supplier Personnel require an on-going security review to ensure no conflicts of interest emerge from the case material being processed and Suppliers should consider active support to those dealing with sensitive, and often graphic, materials.
PRI/R/SPECIAL/04	The Supplier Personnel access the Customer's secure network to retrieve and post completed scanned work to an indexed folder structure in order that the Data does not leave the Customer System.
PRI/R/SPECIAL/05	The combination of paper and electronic records may need repagination and indexing to complete the task.
PRI/R/SPECIAL/06	The digital output is preferred to be on password protected media, such as USB flash drive, with password sent via email once media is received by the Unit requesting.
PRI/R/SPECIAL/07	The digital output (PDF) must have 'text search' scope.
PRI/R/SPECIAL/08	Unless otherwise requested by the Customer, the Supplier Solution shall be capable of: a. Scanning material at the supplier's off-site scanning facility;

#	**Requirement**
	b. Returning the originals once scanned to a storage site as instructed by the Customer; c. Allowing Customer staff to index the scanned output.
PRI/R/SPECIAL/09	The Supplier shall perform an initial scan of a subset of the pages to be scanned and have the Customer endorse the quality of the subset first, before proceeding with the scanning of all the material to be scanned.

4.3 Non Functional Requirements

4.3.1 Supportability

#	**Requirement**
PRI/R/SUPPORT/01	The Supplier shall ensure support and maintenance of the hardware and Software which make up the Supplier Solution (shall, where reasonably possible), be co-terminus with the Call Off Contract.
PRI/R/SUPPORT/02	The Supplier Solution shall demonstrate corporate social responsibility by lowering the carbon cost when compared to the current infrastructure for the equivalent capacity.
PRI/R/SUPPORT/03	The Supplier's supply chain shall demonstrate the use of 'Green IT' throughout the duration of the Call Off Contract.
PRI/R/SUPPORT/04	The Supplier Solution shall, where practicable, use CE marked components from reputable manufacturers that conform to the appropriate Standards and Regulations specified.

4.3.2 Capacity Planning & Management

#	**Requirement**
PRI/R/CAPPLAN/01	The Supplier shall be responsible for the development and expansion of all Services provided under this Call Off Contract.
PRI/R/CAPPLAN/02	The Supplier shall define and agree forecast and deployment processes with the Customer.
PRI/R/CAPPLAN/03	The Supplier shall monitor, analyse and report to Customer on capacity volumes and trends.

4.3.3 Service Performance Reporting

#	**Requirement**
PRI/R/SERPERF/01	The Supplier shall provide regular and comprehensive Service Performance Monitoring Reports on achievements and trends against Service Levels and on Incidents and issues arising during the previous Service Period. These reports shall provide sufficient information presented in a structured format to enable easy reconciliation with the Supplier's invoices and shall include, as a minimum, monthly figures (against Service Levels) and trends for: • Service availability and performance; • Incident management including details of Incidents Resolved; outstanding Incidents and the steps being taken to effect permanent solutions and fix times for the different Severity Levels of Incidents; • Alerts during reporting period; • Capacity and usage reports (monthly and trend analysis); The design of the reports, based on the content identified above, shall be agreed by the Parties during Implementation. The Customer shall retain the right to vary the design and content of such reports thereafter and, if there is any impact to the monthly reporting cycle, the Parties shall discuss and agree any adjustments, as applicable. The Customer reserves the right to challenge the information received and the Supplier shall respond to those challenges in a timely manner as directed by the policies, processes and procedures or otherwise.
PRI/R/SERPERF/02	The Supplier shall produce a Monthly Service Performance Monitoring Report which shall be delivered within 5 Working Days of the Service Measurement Period.
PRI/R/SERPERF/03	The Supplier shall produce a Monthly Finance Report which shall be delivered within 8 Working Days of the end of the Service Measurement Period.

4.3.4 License Management

#	**Requirement**
PRI/R/LICENSE/01	The Supplier shall maintain a clearly defined Software policy, to ensure that when new or additional Software purchases are made by the Supplier, checks are made on:

#	**Requirement**
	• the availability of un-utilised Software that has already been purchased; • the existence of corporate licence or other such agreements or facilities; and • the need for all Software in use to be legitimately licensed. For Software supplied by the Customer: • the Supplier shall record, maintain and monitor operational details relating to usage.
PRI/R/LICENSE/02	For Software provided by the Supplier, the Supplier shall monitor the number and type of Licenses in use for all such Software ensuring all Software in use is legitimately licensed. The Supplier will notify the Customer of any unlicensed Software that is identified and shall delete any such Software, when instructed to do so by the Customer. For Transferring in Software: the Supplier shall record, maintain and monitor operational details relating to usage; and the Supplier shall ensure optimum use is made of all Software, both current and legacy, for which licences are held.

4.3.5 Hardware and Software Asset Management

#	**Requirement**
PRI/R/ASSET/01	The Supplier shall record all hardware and Software on the Supplier's CMDB
PRI/R/ASSET/02	The Supplier shall record, maintain and monitor all installed Software and associated licence details.
PRI/R/ASSET/03	As hardware and Software changes, the Supplier shall record the changes within the Supplier's CMDB, and provide the Customer with monthly updates to the Supplier's CMDB.
PRI/R/ASSET/04	The Supplier shall provide regular hardware and Software asset reports to the Customer. The format and frequency of these reports to be agreed during Implementation.

4.3.6 Application upgrade and decommissioning

#	**Requirement**
PRI/R/APPS/01	The Supplier shall work with the Customer, and the Other Suppliers, for the managed upgrade or decommissioning of any Application that forms part of the Supplier Solution, including interfaces, scripts and application data.
PRI/R/APPS/02	The Supplier shall ensure the integrity of data relevant to the Application is tested prior the Application upgrade.

4.3.7 Customer Satisfaction

#	**Requirement**
PRI/R/CUSTSAT/01	The Supplier shall adhere to and operate in accordance with Complaint Management Policies, Processes and Procedures as directed by the Customer. The Supplier shall have agreed procedures for recording and responding to Customer complaints and shall ensure that all complaints are reported in Performance Monitoring Report to the Customer.
PRI/R/CUSTSAT/02	The Supplier shall assist and co-operate with the Customer in defining and conducting regular Customer satisfaction surveys of the Services they provide and shall have procedures, agreed with the Customer, for responding to any negative output from these surveys.

4.3.8 SERVICE DESK - Customer / User Satisfaction

#	**Requirement**
PRI/R/USERSAT/01	The Supplier shall support the Customer in identifying and implementing methods of assessing Customer satisfaction for the services that form part of this Call Off Contract.
PRI/R/USERSAT/02	The Supplier shall, as a minimum, utilise their experience and expertise to recommend improvement actions required to increase Customer satisfaction rates.

4.3.9 Equipment Maintenance and Disposal

#	**Requirement**
PRI/R/EQUIP/01	The Supplier shall maintain and support its Equipment in accordance with the recommendations of the relevant OEM. Such maintenance and support shall include: • upgrades and revisions to Hardware, Software and firmware • corrective maintenance • configuration management of Equipment • asset management of Equipment.
PRI/R/EQUIP/02	The Supplier shall proactively undertake remote management and monitoring of the supported Equipment in accordance with the appropriate security accreditation.
PRI/R/EQUIP/03	The Supplier shall develop and implement an agreed Equipment Management Policy to include: • upgrades and revisions to hardware, Software and firmware • corrective maintenance • configuration management of Equipment • asset management of Equipment.
PRI/R/EQUIP/04	Provided that prior written approval is given by the Customer, the Supplier shall de-install and remove any assets as necessary.
PRI/R/EQUIP/05	The Supplier shall bear the costs relating to decommissioning, collection and disposal of any Assets and Equipment when they are no longer required
PRI/R/EQUIP/06	The Supplier shall ensure that the Policy, Process and Procedures related to the holding of spares will be reflected in the Supplier's Equipment Management Policy, and advise the Customer on the level of all spares that need to be held such that Service Levels can be met.
PRI/R/EQUIP/07	The Supplier shall ensure that sufficient spares are held to maintain and deliver the Services, in accordance with the Service Levels.
PRI/R/EQUIP/08	The Supplier shall ensure that configuration details of spares are held within the Supplier's Configuration Management Database (CMDB), such that the CMDB differentiates the details held as spares.

4.3.10 Site Surveys

#	**Requirement**
PRI/R/SSURVEY/01	The Supplier shall conduct Site surveys for any ad-hoc requirements within five (5) Working Days of a formal request being received from the Customer.

#	**Requirement**
PRI/R/SSURVEY/02	The Supplier shall co-operate with the Customer, and Other Suppliers to determine printer related dependencies on Other Suppliers, and list them in the Change Request Impact Assessment for the site survey.

Testing

#	**Requirement**
PRI/R/TESTING/01	The Supplier shall ensure that all Testing is conducted in accordance with the provisions of Call Off Schedule 5 (Testing).

4.3.11 Print Capacity management

#	**Requirement**
PRI/R/CAPMGT/01	The Supplier shall conduct on-going monitoring of capacity and trend analysis of print device utilisation.

5 SECURITY

The requirements set out under this section cover:

#	**System**
5.1	General Security;
5.2	Physical Security;
5.3	Architecture Security;
5.4	Encryption
5.5	Environment Protective Monitoring;
5.6	Environment Identity and Access Management
5.7	Anti-Virus and Malware
5.8	Vulnerability Management
5.9	Remote Access Security

In the event that there is a conflict between this section and the information contained within Call Off Schedule 7 (Security), this section shall take precedence.

5.1 General Security

#	**Requirement**
PRI/R/GENSEC/01	The Supplier shall ensure compliance with all applicable UK Government / HMG Cyber Security Policy including, but not limited to, the Security Policy Framework (SPF) and Government's Minimum Cyber Security Standard.
PRI/R/GENSEC/02	The Supplier shall comply with all aspects of the Customer's Security Assurance Strategy and associated approach and produce all required assurance documentation in the required format and to Customer specified timescales.
PRI/R/GENSEC/03	The Supplier shall have Cyber Essentials Certification. It is desirable, but not essential, that the Supplier is working toward Cyber Essentials Plus
PRI/R/GENSEC/04	The Supplier shall have ISO27001 Certification.
PRI/R/GENSEC/05	The Supplier shall provide the Customer access to Supplier Personnel and Supplier premises as required for the purposes of improving and auditing security.
PRI/R/GENSEC/06	The Supplier shall operate a Protective Security Monitoring regime that collects security event related information across the entirety of

#	**Requirement**
	the solution provided. This information shall be correlated and analysed in order that the Supplier can take pro-active intervention action when concerns are identified.
PRI/R/GENSEC/07	The Supplier shall ensure that named User accounts used by the Supplier Personnel for support, administration and management shall have specific roles/privileges. Generic unnamed administrative accounts will not be allowed unless explicitly authorised by the Customer's Departmental Security Unit.
PRI/R/GENSEC/08	The Supplier shall ensure that all equipment used to support the Supplier Solution shall be sufficiently secure from tampering and shall alert in the event of attempted tampering on the basis that the information carried is protectively marked no higher than OFFICIAL-SENSITIVE.
PRI/R/GENSEC/09	The Supplier shall provide the results from the Supplier's protective monitoring solution to the Customer (or an approved agent of the Customer) for central review and analysis, in order to allow for oversight of the totality of the Customer's security monitoring arrangements at a single point. The Supplier will retain responsibility for all monitoring and necessary intervention requirements associated with the service provided. The Supplier shall ensure that information is provided in a format that is compatible with any tools that are deployed centrally on behalf of the Customer and in an agreed timescale.
PRI/R/GENSEC/10	The Supplier shall be responsible for the scope and delivery of IT Health checks / Penetration Testing to the satisfaction of the Customer. The Supplier shall offer necessary assistance should the Customer determine that they require additional / independent IT Health checks as frequently as reasonably required by the Customer. All IT Health checks / Penetration Testing shall be delivered by a CHECK 'Green' penetration testing service provider.
PRI/R/GENSEC/11	The Supplier shall make available their Security Management Plan as and when required by the Customer and keep it up to date.

5.2 Physical Security

#	**Requirement**
PRI/R/PHYSEC/01	The Supplier shall operate policies and procedures for all physical Sites deployed for the solution to support the operation of a safe and secure working environment in offices, rooms, facilities, and secure areas processing Customer Data.
PRI/R/PHYSEC/02	The Supplier shall ensure that all Assets operated by the Supplier to support the Supplier Solution must be classified in terms of business criticality, service-level expectations, and operational

#	**Requirement**
	continuity requirements. The Supplier shall maintain and keep updated regularly a complete inventory of all assets utilised and assigned ownership by defined roles and responsibilities.
PRI/R/PHYSEC/03	The Supplier shall deploy a combination of physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance (including CCTV), physical authentication mechanisms, reception desks, and security patrols) to safeguard Customer Data.
PRI/R/PHYSEC/04	The Supplier shall control and monitor access to areas that could facilitate access to Customer Data or services by physical access control mechanisms to ensure that only authorised Supplier Personnel are allowed access.
PRI/R/PHYSEC/05	The Supplier shall manage access to all of its sites, such as service areas and other points where unauthorised personnel may enter the premises. These shall be monitored, controlled and isolated from systems processing Customer Data and services to prevent unauthorised data corruption, compromise, and loss. Authorisation shall be obtained from the Customer prior to relocation or transfer of any element of the print solution to offsite / alternative premises.

5.3 Architecture Security

#	**Requirement**
PRI/R/ARCSEC/01	The Supplier shall ensure that the architecture to support the print solution for the Customer undergoes an accreditation / assurance process in accordance with the Customer's Accreditation / Assurance Strategy.
PRI/R/ARCSEC/02	The Supplier shall ensure architecture design is undertaken in accordance with NCSC's Cyber Security Design Principles.
PRI/R/ARCSEC/03	The Supplier shall develop, implement and maintain a security governance framework that coordinates and directs its overall approach to the management of services to be delivered (e.g. ISO27001 registration / certification, NIST or similar).
PRI/R/ARCSEC/04	The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and access to the minimum possible level) to the design and configuration of print resources that will process Customer Data.
PRI/R/ARCSEC/05	The Supplier shall ensure that any transmission of Customer Data is adequately protected against tampering, denial of service, eavesdropping and virus ingress.

#	**Requirement**
PRI/R/ARCSEC/06	The Supplier shall ensure that its Supplier Personnel are subject to: (i) adequate personnel security screening; and (ii) adequate security education to ensure that they are able to perform their role.
PRI/R/ARCSEC/07	The Supplier shall design and develop services to identify and mitigate threats to security and any risks that such threats may present to Customer Data.
PRI/R/ARCSEC/08	The Supplier shall ensure that its supply chain supports (to the satisfaction of the Customer) all of the security principles that the print solution is required to implement.
PRI/R/ARCSEC/09	The Supplier shall ensure that, where applicable, the Customer is provided with the tools required to take appropriate action on any issues or risks that may arise (such as, access to audit and log information to support Incident investigation). The Supplier shall ensure that a forensic readiness capability is consistently provisioned that is aligned with recognised best practice and is appropriate to the sensitivity of data processed on behalf of the Customer.
PRI/R/ARCSEC/10	The Supplier shall be responsible for security hardening of all print infrastructure. Operating systems shall be hardened to provide only necessary ports, protocols, and services to meet Customer business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard.
PRI/R/ARCSEC/11	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is embedded within the solution and at its perimeter and interfaces with any other network, service, applications or devices.
PRI/R/ARCSEC/12	The Supplier shall provide boundary controls within the print infrastructure and identify and confirm the security of all connectivity aspects associated with services provisioned for the Customer. Separation and segregation shall be achieved by a combination of physical and technical arrangements that have been approved by the Customer to ensure there is no likelihood of Customer Data being corrupted or exposed to unauthorised people.
PRI/R/ARCSEC/13	Access to all management functions or administrative consoles for print components involved in the processing of Customer Data shall be restricted to authorised personnel, based upon the principle of least privilege and supported through technical controls.
PRI/R/ARCSEC/14	The Supplier shall ensure that access to all Service interfaces is limited to authenticated and authorised End Users only.
PRI/R/ARCSEC/15	The Supplier shall establish a change and configuration control process for the print environment to: a. Prevent installation of unauthorised Software;

#	**Requirement**
	b. Update & patch known security vulnerabilities in a timely manner; c. Test all patches and updates prior to deployment; d. Implement work-rounds / other controls where delays in fixing vulnerabilities occur.
PRI/R/ARCSEC/16	The Supplier shall: a. Provide the Customer with all Customer Data on demand in an agreed open format; b. Have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade; c. Securely destroy all media that has held Customer Data at the end of life of that media in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or latest guidance produced by NCSC / Government); and Securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or latest guidance produced by NCSC / Government).
PRI/R/ARCSEC/17	The Supplier shall make available to the Customer and its designated agents any reasonably requested resources including physical access to Sites, facilities and Key Personnel that support the delivery of the Services.
PRI/R/ARCSEC/18	The Supplier where applicable, shall adhere to and support compliance with, all relevant 'Codes of Connection' for services accessed by the Customer.
PRI/R/ARCSEC/19	The Supplier recognises the need for information to be safeguarded under the Data Protection Legislation and related guidance . To that end, the Supplier shall be able to state to the Customer the physical locations in which data may processed from, or transmitted via, and to confirm that all relevant legal and regulatory frameworks are complied with.
PRI/R/ARCSEC/20	The Supplier shall develop a Business Continuity Plan (BCP) and Disaster Recovery arrangements incorporating risks identified in a risk assessment, including malicious, accidental, technical failure and natural events that could disrupt the Customer's business that is reliant upon the services provided by the Supplier's print environment. The plans shall reflect Customer Recovery Time Objectives (RTOs).

5.4 Encryption

#	**Requirement**
PRI/R/ENCRYP/01	Any Customer Data transmitted over non-approved / non-assured networks (including the Internet, mobile networks or un-protected enterprise network) shall be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC.

5.5 Protective Monitoring

#	**Requirement**
PRI/R/PROTECT/01	The Supplier shall deliver a Protective Monitoring regime that is consistent with NCSC guidance on Security Monitoring.
PRI/R/PROTECT/02	The Supplier's Protective Monitoring regime shall provide centralised collection, analysis and correlation of information that is generated by security enforcing technologies such as firewalls, IDS/IPS, AV logs etc. that relate to the print arrangements provided for the Customer.
PRI/R/PROTECT/03	The Supplier shall align its Protective Monitoring regime for day-to-day business service provision with *CESG GPG13 – Protective Monitoring for HMG ICT Systems*. GPG13 is an archive document, so its content should be used to 'baseline' the approach driven by the focus and relevance of Protective Monitoring Controls (PMCs) contained within the document.

5.6 Identity and Access Management

#	**Requirement**
PRI/R/ACCESS/01	The Supplier shall operate access control policies and procedures and supporting business processes and technical measures, for ensuring appropriate identification and authentication of personnel involved in the administration of the print environment.
PRI/R/ACCESS/02	The Supplier shall define procedures and confirm roles and responsibilities for provisioning and de-provisioning of administrative User accounts following the rule of least privilege, based on defined job function.
PRI/R/ACCESS/03	The Supplier shall provide account management, delivering the following: • A centralised process to authorise the creation and deletion of all accounts; • Full visibility (to authorised personnel) in a single place, on who has access to which resource;

#	**Requirement**
	• Ability to ensure that proposed new End Users do not already have accounts already created.
PRI/R/ACCESS/04	The Supplier shall ensure that 'authentication' is risk based and supported by a centralised policy framework. The policy framework shall allow for the deployment of multi-factors for authentication, which can be augmented as a result of the sensitivity and/or risk to the print environment at any given time.
PRI/R/ACCESS/05	The Supplier shall identify, assess, and prioritise risks associated with any third-party access to the print environment by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorised or inappropriate access. Risk management controls shall be implemented prior to providing access to any third party.
PRI/R/ACCESS/06	The Supplier shall ensure timely de-provisioning of access to the print environment in accordance with established policies in the event of change to a user's status (e.g., termination of employment or other business relationship, job change, or transfer).
PRI/R/ACCESS/07	The Supplier shall provide centralised administration of the Identity and Access Management regime for the print environment. Centralised administration shall deploy management tools in order to have complete visibility of the Identity and Access Management regime.
PRI/R/ACCESS/08	The Supplier shall ensure that all End Users are managed through a centralised policy driven approach. Privileges shall be allocated and managed using a centralised management facility, which provides visibility and control of systems and services that access has been granted to.
PRI/R/ACCESS/09	The Supplier shall implement an Identity and Access Management regime that deploys a centralised function to monitor and report activity including: a. Suspicious login attempts / failed logins; b. Monitor access patterns; c. Allowing for tailored and scalable monitoring of End Users / activities when required; d. Identify unknown / unrecognised access devices and locations; e. Centralised logging and analysis of 'security events'.
PRI/R/ACCESS/10	The Supplier shall ensure that access to, and use of, audit tools that support the operation of the print environment's identity and access management regime shall be appropriately segregated and access

#	**Requirement**
	restricted to prevent inappropriate disclosure and tampering of log data.
PRI/R/ACCESS/11	The Supplier shall implement a regime that maintains security and event related information in a manner that ensures forensic integrity is retained. Arrangements shall support swift intervention following the identification of an Incident, which allows for example, immediate suspension of an account across all instance of its use. The Supplier shall be responsible for integration into wider Customer Incident response procedures, in order to ensure a consistent response irrespective of Incident type.

5.7 Anti-Virus and Malware

#	**Requirement**
PRI/R/ANIMAL/01	The Supplier shall ensure that the Services the Supplier provides under this Call Off Contract are protected through an holistic anti-virus and malware prevention and detection regime that delivers layered security against this threat.
PRI/R/ANIMAL/02	The Supplier shall ensure that the anti-virus and malware prevention and detection regime is applied both within the print environment and at its perimeter and interfaces with any other network, service, application or device.
PRI/R/ANIMAL/03	The Supplier shall employ automated tools to continuously monitor all services that are provisioned within the environment for virus and all forms of malware. All malware detection events shall be centrally collated, managed and logged.
PRI/R/ANIMAL/04	The Supplier shall maintain the anti-virus and malware prevention and detection regime so that it is updated in accordance with extant threat levels. Updates to Software supporting the regime shall take place on both a scheduled and threat informed basis.
PRI/R/ANIMAL/05	The Supplier shall ensure that updates to the malware prevention and detection regime are pushed out to all services that are provisioned within the scope of the service provided in a consistent and timely manner.
PRI/R/ANIMAL/06	The Supplier shall ensure that its process to download and distribute updates to the anti-virus malware prevention and detection regime does not introduce threats to wider operating environment. The Supplier shall ensure that all updates are verified and are free from malicious content prior to introduction to the environment.

#	**Requirement**
PRI/R/ANIMAL/07	The Supplier's malware prevention and detection regime shall be integrated with the Customer's wider Incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.

5.8 Threat and Vulnerability Management

#	**Requirement**
PRI/R/VULMAN/01	The Supplier shall deliver a Vulnerability Management regime that provides assurance to the Customer that all potential new threats, vulnerabilities or exploitation techniques, which could affect the print environment are assessed and corrective action is taken.
PRI/R/VULMAN/02	The Supplier shall monitor relevant sources of information relating to threat, vulnerability and exploitation techniques, in order to support the provision of an appropriately informed Vulnerability Management regime.
PRI/R/VULMAN/03	The Supplier shall consider the severity of threats taking full account of the criticality of Customer Data in the prioritisation of mitigation implementation.
PRI/R/VULMAN/04	The Supplier shall track all identified vulnerabilities and monitor them until required mitigations have been deployed. Timescales for implementing mitigations to vulnerabilities found within the print environment shall be communicated to the Customer.
PRI/R/VULMAN/05	The Supplier shall act immediately to put mitigations in place for any vulnerability where evidence suggests that it is being exploited 'in the wild'. If there is no evidence that the vulnerability is being actively exploited, and where there is no vendor recommendation then the following timescales shall be considered minimum good practice (see Cyber Essentials): *'Critical' or 'high risk' patches deployed within 14 calendar days of a patch becoming available.*
PRI/R/VULMAN/06	The Supplier shall provide 'real time' vulnerability scanning and remediation deploying best-in-class Vulnerability Management solutions that deliver comprehensive discovery, tailored to the modern, constantly evolving threat environment.
PRI/R/VULMAN/07	The Supplier shall provide a Vulnerability Management regime that includes within its scope, all assets that fall within the scope of the print service being provisioned.

#	**Requirement**
PRI/R/VULMAN/08	The Supplier shall undertake appropriate Root Cause analysis of identified vulnerabilities, in order to learn from the mitigation process, to limit the possibility of recurrence. This shall contribute to a pro-active approach to Vulnerability Management that is not limited to simply responding to events.
PRI/R/VULMAN/09	The Supplier's Vulnerability Management regime shall be integrated with the Customer's wider Incident response and management processes to support appropriate visibility and consistency of response across the multi-supplier service environment.

5.9 Remote Access

#	**Requirement**
PRI/R/REMOTE/01	Where remote access is required to the print solution, the Supplier shall provide this in accordance with NCSC guidance taking account of both platform and device specific guidance.
PRI/R/REMOTE/02	The Supplier shall provide assured data-in-transit protection. This shall be achieved through the deployment of a VPN. NCSC recommends the deployment of always on, IPsec VPN, which routes traffic through a remote network for inspection. This and other guidance provided by NCSC relating to protocols and cryptography shall be adhered to in the design of the remote access solution.
PRI/R/REMOTE/03	The Supplier shall provide assured data-at-rest protection. Any Customer data or technical data relating to the print environment stored on remote access devices shall be encrypted with an encryption product that is assured to 'Foundation Grade' under NCSC's Commercial Product Assurance (CPA) scheme. This shall be deployed when the device is in its 'rest' state. For 'always on' devices, this encryption shall be deployed when the device is locked.
PRI/R/REMOTE/04	The Supplier shall deploy an effective authentication process for all devices and the services they provide access to, which should include the following aspects: • User to device, whereby the End User shall only be granted access to the device following successful authentication to the device; • User to service, whereby the End 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.

#	**Requirement**
PRI/R/REMOTE/05	The Supplier shall deploy 'malicious code detection and prevention' controls for the remote access service. Arrangements shall detect, isolate and defeat malicious code, which may have achieved ingress to the remote access architecture.
PRI/R/REMOTE/06	The Supplier shall ensure effective 'security policy enforcement' to ensure that policies set by the enterprise are implemented in remote access devices. It shall be possible to centrally enforce a set of security policies on devices and ensure that these policies cannot be circumvented by the device user or unauthorised entity.
PRI/R/REMOTE/07	The Supplier shall deploy 'external interface protection' ensuring that remote access devices are limited to an agreed profile, the number of ports (physical and logical) and services exposed to untrusted networks and devices.
PRI/R/REMOTE/08	The Supplier shall deploy 'event collection' for all elements of the remote access service, to report security events to a centrally provisioned audit and monitoring arrangement. This facility shall be restricted from the remote access user and mitigate against unauthorised access attempts.
PRI/R/REMOTE/09	The Supplier shall deploy an 'Incident response' arrangement that integrates with wider response procedures in place across the Customer ICT Environment.

5.10 Information Technology Accessibility (ITA)

#	**Requirement**
PRI/R/ITA/01	The Supplier shall provide print devices to meet the accessibility requirements of End Users who require specialist print equipment as approved by the Customer.
PRI/R/ITA/02	The Supplier shall ensure power packs, cables, toners and all other relevant components and peripherals, have been acquired, prior to attempting a print device installation for an ITA End User.
PRI/R/ITA/03	The Supplier to provide a configuration report as part of every print device installation, and this report is to be provided to the Customer's nominated representative (to be nominated during the Implementation phase) (Clarification: The report is to be provided directly to one of the Customer's Other Suppliers, with no expectation of the Customer's End User being required to do this.)

#	**Requirement**
PRI/R/ITA/04	Upon the successful installation of a print device, the Supplier shall successfully test all of the functions of the newly installed print device before the device installation can be deemed complete.

6 CATEGORY–3 - CUSTOMER'S MULTI-SUPPLIER ENVIRONMENT REQUIREMENTS

The Supplier acknowledges that it is providing the Services and the Deliverables to the Customer within a multi-vendor environment, where co-operation between Supplier and Other Suppliers is critical to the effectiveness of the Customer's operations and critical government functions. The Supplier therefore agrees to sign (when notified by the Customer to do so) and comply with the terms of the Co-Operation Agreement contained at Annex 1 to Part B of Call Off Schedule 18 (Governance and Cooperation) during the Call Off Contract Period. The Customer confirms to the Supplier that it has entered into agreements with its Other Suppliers for the provision of services and other deliverables that contain co-operation agreements on terms that are no less restrictive than the terms of that Co-Operation Agreement.

The Customer is entitled to appoint an Agency Manager to act on the Customer's behalf at any time during the Call Off Contract Period and the Supplier shall comply with the Customer Requirements set out in this Category 3.

The Agency Manager will be carrying out certain contract administration activities (including change management, verification of invoices and payment, etc., as applicable) and supplier relationship management in connection with this Call Off Contract. The Supplier shall work with, respond to, cooperate with and assist the Agency Manager and, if directed by the Agency Manager, Other Suppliers in relation to such contract administration and supplier relationship management.

The Agency Manager service requirements set out in the relevant contracts between the Customer and its Other Suppliers are intended to facilitate the Supplier to fulfil the Supplier's obligations relating to interfacing, working with and complying with the instructions and requirements of the Agency Manager under this Call Off Contract, including utilising and aligning the Services and the delivery and performance of the same with the Policies, Processes, Procedures (PPP) of the Agency Manager.

The requirement to co-operate with the Customer, Agency Manager and Other Suppliers is set out under the following ITIL headings:

a. Service Desk
b. Incident Management
c. Request Management
d. Problem Management
e. Access Management
f. Change Management
g. Asset and Configuration Management (SACM)
h. Knowledge Management
i. Service Implementation
j. Continual Service Improvement

6.1 Service Desk

#	**Requirement**
PRI/R/DESK/01	The Supplier shall adhere to: (i) the Customer's service desk Policies, Processes and Procedures; and (ii) guidance on interfacing with the Service Desk as provided to the Supplier by the Customer.

#	**Requirement**
PRI/R/DESK/02	The Supplier shall interface with the Service Desk such that the Supplier is able to access the Customer's ITSM, receive Incident records logged by the Supplier, Other Suppliers and End Users, to update, amend and pass back Incident records to the Service Desk as necessary.
PRI/R/DESK/03	The Supplier shall interface with the Service Desk such that the Supplier is able to access the Customer's ITSM, receive Service Catalogue requests logged by the Supplier, Other Suppliers and End Users, to update, amend and pass back request related records to the Service Desk as necessary.
PRI/R/DESK/04	The Supplier shall ensure that, where necessary, the interfaces between the Supplier Systems and the Service Desk shall be automated to allow tickets to be raised automatically between the Supplier Systems and the Customer ITSM.
PRI/R/DESK/05	The Supplier shall agree the parameters surrounding the generation of automatic tickets at the Customer's ITSM with the Customer during Implementation.
PRI/R/DESK/06	The Supplier Solution shall enable Incidents allocated to the Supplier by the Service Desk to be accepted twenty four (24)/Seven (7). The above statement of Service Desk availability shall be known as the "**Service Desk Hours**".
PRI/R/DESK/07	The Supplier shall contribute to the Knowledge Management System and the Known Error Log provided by the Customer to support improved Incident analysis.
PRI/R/DESK/08	The Supplier shall provide feedback to End Users and /or the Customer on progress made with resolving an Incident. Such feedback shall include: (i) advice on any remedial action being taken; (ii) the estimated date and time when the Incident may be resolved; (iii) and advice allowing the End User to continue to use the Services until such time as the Incident is resolved.
PRI/R/DESK/09	The Supplier shall ensure that Root Causes to Incidents and Problems are addressed.

6.2 Incident Management

#	**Requirement**
PRI/R/INCMAN/01	The Supplier, using a Resolver Group as appropriate, shall investigate and resolve all Incidents in accordance with the Service Levels, including: • assessing the probable Root Cause of each Incident;

#	**Requirement**
	• testing and replacing or repairing faulty hardware/Software as required in order to Achieve first time fix or full Incident Resolution; • carrying out any other procedures as required to facilitate the resolution of the Incident; and • the routine reporting of Incident Resolution, through the Performance Monitoring Report, to identify a first time fix and full Incident Resolution.
PRI/R/INCMAN/02	Suppliers should proactively monitor their equipment and identify failures. These should be created as Incidents and dealt with appropriately.
PRI/R/INCMAN/03	The Supplier shall work with the Customer and Other Suppliers to ensure that, prior to arranging a visit to a Home Worker, Broadband Services to that Home Worker's location is functioning properly.
PRI/R/INCMAN/04	The Supplier shall participate with the Customer in Incident Reviews and Major Incident Reviews, as necessary.
PRI/R/INCMAN/05	The Supplier shall promptly complete agreed corrective actions as agreed with the Agency Manager.
PRI/R/INCMAN/06	The Supplier shall promptly notify the Customer of any Incident that is known to have breached or is likely to breach the Service Levels or that has, in the opinion of the Supplier, been incorrectly allocated.
PRI/R/INCMAN/07	The Supplier shall; (i) update the Incident record with all relevant information to ensure that Root Cause Analysis can be carried out by the Customer; and (ii) co-operate with the Customer and Other Suppliers as required to carry out Root Cause Analysis.
PRI/R/INCMAN/08	The Supplier shall (i) contribute to Major Incident reports; and (ii) ensuring that Major Incident reports provide complete details to the Customer; and (iii) ensure that the reason for the breach of the Service Level(s) is recorded and agreed with the Customer.
PRI/R/INCMAN/09	Where the Agency Manager has altered the assigned Incident Severity Level of an Incident in accordance with Customer instructions and agreed this with the Supplier, the Supplier shall resolve such Incident in accordance with the new Incident Severity Level.
PRI/R/INCMAN/10	The Supplier shall ensure that, in the event that the investigation of an Incident reveals weaknesses or flaws in the Supplier Solution, then any Change required by the Supplier to rectify the weakness or flaw must be Approved by the Customer, in advance and implemented via Change Control. For the avoidance of doubt, the Change to the Supplier Solution shall be at no cost to the Customer.

#	**Requirement**
PRI/R/INCMAN/11	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, temporary fix or aid escalation to the relevant Resolver Group.
PRI/R/INCMAN/12	The Supplier shall use the Customer's configured ITSM, which contains the Supplier's Service Levels, to track the elapsed time during the life cycle of the Incident and its resolution, and shall provide resolution updates 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 and to the Agency Manager.
PRI/R/INCMAN/13	The Supplier shall be responsible for ensuring a resolution or Workaround is provided as quickly as possible in order to restore the service to End Users with minimum disruption to their work.
PRI/R/INCMAN/14	The Supplier shall ensure the efficient escalation of Incidents to the Service Desk where additional or alternative knowledge is required to resolve the Incident.
PRI/R/INCMAN/15	The Supplier shall co-operate and support the work of the Service Desk suppliers' Major Incident Management (MIM) Team to ensure that its Resolver Group, and other relevant Resolver Groups, provide: • a single point of contact for Major Incidents; • a detailed breakdown of the Incident; • estimated resolution delivery timescale; • resources to participate in Multi-Supplier technical discussions, as required, and confirm the approach with the MIM Team; and resources to implement the agreed actions and update the MIM record with progress and the ongoing status at pre-agreed frequency.
PRI/R/INCMAN/16	The Supplier shall progress all Incidents assigned to the Supplier via the Customer's ITSM (ServiceNow) tool as per the time line driven by the Severity Level assigned to the Incident. Where a Resolution requires the Supplier to attend any Customer Premises, the Supplier will despatch an engineer to the relevant Customer Premises at the earliest opportunity based on the relevant location's opening and closing times***.***

6.3 Request Management

#	**Requirement**
PRI/R/REQMAN/01	The Supplier shall contribute to and use the Customer supplied Business Service Catalogue.
PRI/R/REQMAN/02	The Supplier shall review all management information on a monthly basis to identify trends or significant changes or increases in service request volumes, for discussion with the Customer and, where necessary, Other Suppliers, as applicable.
PRI/R/REQMAN/03	The Supplier shall identify possible Process improvements and promptly make appropriate recommendations to the Customer in writing.
PRI/R/REQMAN/04	The Supplier shall immediately bring to the attention of the Customer any issues that prevent the Supplier from processing Service Requests. (Clarification: This activity should include providing the roadmap of Devices and the early warning of Devices which are to go end-of-life, and the substitution of equivalent models after adequate testing.)
PRI/R/REQMAN/05	The Supplier shall ensure that Service Requests received from the Customer are expedited within agreed Service Levels when assigned by the Service Desk
PRI/R/REQMAN/06	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Customer in response to a Service Request raised in the Customer ITSM.
PRI/R/REQMAN/07	The Supplier shall: (i) co-operate with the Customer to proactively manage and monitor the status and progress of all Service Requests for the Services ordered via the Business Service Catalogue; and (ii) adhere to the Customer's PPP relevant to Service Requests.
PRI/R/REQMAN/08	The Supplier shall respond to the Customer or the Customer's enquiries regarding Service Requests with accurate and up-to date information.

6.4 Problem Management

#	**Requirement**
PRI/R/PROB/01	The Supplier shall accept appropriately assigned Problems from Service Desk, and bring to the attention of the Service Desk as soon as is practicable, any inaccurately assigned Problems that should be assigned to Other Suppliers.
PRI/R/PROB/02	The Supplier shall assist and co-operate with the Customer to identify, prioritise and manage through to resolution all Problems assigned to the Supplier that cause or have the potential to cause disruption to the Customer's business.

#	**Requirement**
PRI/R/PROB/03	The Supplier shall assist and co-operate with the Customer in and participate in conducting Root Cause Analysis and will ensure that records of Problems are updated to reflect the agreed outcome of such analysis.
PRI/R/PROB/04	The Supplier shall assist the Customer by reviewing management information on a Monthly basis; and produce expert trend analysis and management summaries to identify trends or significant changes or increases in Problem volumes, for discussion with the Customer and Other Suppliers at the appropriate forums.
PRI/R/PROB/05	The Supplier shall collate, maintain and provide the Agency Manager accurate and up to date information on Problems, Workarounds and Known Errors, and support the Agency Manager with similar requirements.
PRI/R/PROB/06	The Supplier shall assist and co-operate with the Customer to identify potential Process improvements and make appropriate recommendations to the Customer and Other Suppliers.

6.5 Access Management

#	**Requirement**
PRI/R/ACCMAN/01	The Supplier shall support the Service Desk service supplier's Access Management Service to enable Customer nominated End Users to be able to use the Services.
PRI/R/ACCMAN/02	The Supplier Solution shall adhere to the Customer's Access Management Policies and Procedures and supports Other Supplier's Access Management activities.
PRI/R/ACCMAN/03	The Supplier shall provide appropriate access (including remote access) to enable the Customer to access the Supplier's monitoring tools and systems.
PRI/R/ACCMAN/04	The Supplier shall inform the Customer where it suspects or has reason to believe that inappropriate user access has been obtained.
PRI/R/ACCMAN/05	The Supplier shall assist and co-operate with the Customer and other Suppliers to provide and exchange technical knowledge and support, in order that upgrades, process improvement and Change in both the Supplier's System and Other Supplier's Systems will optimise the benefits of change and mitigate the risk on the services.

6.6 Change Management

#	**Requirement**
PRI/R/CHANGE/01	The Supplier shall contribute to the Change schedule and issue this to the Customer.
PRI/R/CHANGE/02	The Supplier shall contribute to the Release Schedule and associated Release Plan(s) and issue these to the Customer. The Release Schedule will provide details for at least a two Month rolling period.
PRI/R/CHANGE/03	The Supplier shall ensure that vendor recommended patching is applied to all of the Supplier's Equipment and Software used to deliver the Services under this Call Off Contract, as directed by the Customer.
PRI/R/CHANGE/04	The Supplier shall schedule, coordinate and manage planned Service outages in accordance with Policies, Processes and Procedures.
PRI/R/CHANGE/05	The Supplier shall support and assist the Customer by responding to Impact Assessments and shall provide input where required.
PRI/R/CHANGE/06	The Supplier shall monitor, analyse and report to the Customer in respect of Change volumes and trends. The format of such reports shall be agreed during Implementation.
PRI/R/CHANGE/07	The Supplier shall provide all requested management information to the Customer.
PRI/R/CHANGE/08	The Supplier shall raise Change Requests in order to make operational or technical Changes to the Services.
PRI/R/CHANGE/09	The Supplier shall: • attend the Change Advisory Board (CAB) (including emergency CABs as necessary); • ensure that any issues related to the Supplier raised at the Change Advisory Board meeting are progressed to the satisfaction of Customer; and • where required by the Customer, support the progression of Changes owned by Other Suppliers.
PRI/R/CHANGE/10	The Supplier shall track and monitor all approved Changes (within the Customer's ITSM) and ensure that Change records are updated throughout the lifecycle of each Change in accordance with decisions made at the Change Advisory Board.

#	**Requirement**
PRI/R/CHANGE/11	The Supplier shall ensure that Operational Change Requests contain information including, but not limited to: • Implementation Plans; • Test Success Criteria; • Back Out Plans or Remediation Plans; • Plans for handover to support; and • Configuration Items affected.
PRI/R/CHANGE/12	Following Implementation of an Operational Change, the Supplier shall ensure that any post Implementation Period reviews implemented by Customer are carried out and managed effectively, and that any lessons learned from each post Implementation Period review are implemented and fed into the assessment of future Changes.
PRI/R/CHANGE/13	The Supplier shall: (i) identify any potential Change Management process improvements; (ii) make appropriate recommendations to the Customer; and (iii) where these are agreed by the Customer, the Supplier shall manage any process improvement activity until completed.
PRI/R/CHANGE/14	The Supplier shall adhere to the Customer's governance process regarding Change Requests, including): • the raising and recording of Changes; • the assessment and evaluation of the Change; • the cost benefit of the proposed Change; and • the review and closure of Requests for Change (RFCs).

6.7 Asset and Configuration Management (ACM)

#	**Requirement**
PRI/R/ACM/01	The Supplier shall maintain accurate Asset details, including details of the Hardware, operating system and any bespoke or packaged Software.
PRI/R/ACM/02	The Supplier shall carry out Asset disposal; including the procurement of formal certification that secure and environmentally responsible disposal has been conducted, and shall notify the Customer of such disposals, in order for the Agency Manger to maintain the CMDB.
PRI/R/ACM/03	The Supplier shall agree and provide regular reporting to the Customer regarding any relevant licence compliance for all Software used to deliver the Supplier Solution.
PRI/R/ACM/04	The Supplier shall work with the Customer, as required, to confirm the scope of any Asset Management audits and the investigation and resolution of any discrepancies related to Asset Management. Unless agreed otherwise by the Parties, such Asset Management audits shall occur at least once per year during the Initial Period, at no additional Charge to Customer.
PRI/R/ACM/05	The Supplier shall provide the results of Asset Management audit data to the Customer within the timescales and in the format required by the Customer.
PRI/R/ACM/06	The Supplier shall provide CI (Configuration Item) data to the Customer in a format and frequency appropriate for inclusion in the Customer supplied integrated CMDB.
PRI/R/ACM/07	The Supplier shall receive, review and, when instructed by the Customer implement recommendations for Service Asset and Configuration Management process improvements.
PRI/R/ACM/08	The Supplier shall assist and co-operate with the Customer in determining the reason for each Configuration Item discrepancy, its criticality, and actions required to address it.

6.8 Knowledge Management

#	**Requirement**
PRI/R/KNOMAN/01	The Supplier shall contribute to the online knowledge management system provided by the Customer for the capture, storage, and presentation of information required to manage the Services and support the delivery of Other Suppliers' Services.

#	**Requirement**
PRI/R/KNOMAN/02	The Supplier shall ensure that, where data related to the Services is found in the knowledge management system provided by the Customer that is inaccurate, incomplete or lacks integrity, such data is promptly corrected.
PRI/R/KNOMAN/03	The Supplier shall assist and co-operate with the Customer in ensuring the knowledge management system contains data and information, including: • methods to resolve Incidents; • Known Errors; • Service Desk scripts; • build data; • self-help articles; and • frequently asked questions (FAQs).

PART B: SUPPLIER SOLUTION

1. INTRODUCTION

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

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

1.3. Subject to paragraph 1 of Part A of this Call Off Schedule 2, the Supplier shall supply the Supplier Solution to meet the Customer Requirements.

1.4. The detailed provisions of the Supplier Solution to fulfil the Customer Requirements in this Call Off Schedule is set out below:

PART B: SUPPLIER RESPONSE

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