Crown Prosecution Service

CPS Service Desk

Requirements

Functional & Non-Functional

Change Initiative Number: Insert Number/Reference

Project SRO:	[redacted]
Project Manager:	[redacted]
Document Collaborators:	[redacted]

Version	Date	Author	Changes Made
0.1	15/07/22	[redacted]	Initial draft with headings and background info.
0.2	16/07/22	[redacted]	Inserted proposed scope of the service desk. Inserted content for the following sections a. General b. Service Desk availability
0.3	18/07/22	[redacted]	Inserted content for the following sections: 5, 6, 15,19
0.4	21/07/22	[redacted]	Inserted additional content
0.5	22/07/22	[redacted]	Inserted additional content across multiple sections
0.6	27/07/22	[redacted]	Inserted additional content across multiple sections
0.7	28/07/22	[redacted]	Inserted additional content across multiple sections
0.8	15/08/22	[redacted]	Inserted additional content across multiple sections
0.9	23/08/22	[redacted]	Received comments from Cybersecurity team and responded to some of them. Responses prefixed with WZ 23/08
0.10		[redacted]	Reformatted, added new tables and accepted changes.
0.11		[redacted]	Updated scope given by Ric Allen Resolved some comments.
0.12	05/11/[redacted]	[redacted]	1. Updated Glossary 2. Reviewed and accepted changes made in previous version.
0.13	07/11/22	[redacted]	Addressed all review comments provided in Appendix A
0.14	09/11/22	[redacted]	Revised to address a. All of Julie Duffy's comments b. All of Julie's team's comments

			c. Comments arising out of review meeting on 09/11/22
0.15	14/11/22	[redacted]	Revised to address JD, DH, RA comments from meeting on 11/11/22.
0.16	27/11/22	[redacted]	Digital Accessibility review and update, step 1 and step 2 (of 2); any further iterations require DA re-review
0.17	30/11/22	[redacted]	Changed front page. Update following KR, RA, JD & WZ input and amendments. Data Accessibility info kept in but re-ordered in Intro section.
0.18	13/12/22	[redacted]	Updated introduction, reviewed all comments and updated for final review by Debbie Hillary

Contents

1 Glossary

Acronyms	Meaning
1LS	First Line Support
2LS	Second Line Support
3LS	Third Line Support
CMDB	Configuration Management Database
CMS	Case Management System
DA	Digital Accessibility
EUC	End User Compute
DHTML	Dynamic HTML
DPP	Director of Public Prosecution
FTF	First Time Fix
ICT	Information and Communication Technology
ITSM	Information Technology Service Management
IVR	Interactive Voice Response
LAN	Local Area Network
MFD	Multifactor Device
MIS	Management Information System
PP's	Policies and Processes
SLA	Service Level Agreement
SPOC	Single Point of Contact
WAN	Wide Area Network
WMS	Witness Management Service

2 Introduction to the Crown Prosecution Service

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

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

The CPS:

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

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

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

2.1 How we are organised and operate

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

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

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

These three specialist divisions, each headed by a Head of Division (equivalent to a CCP), are:

- International Justice and Organised Crime Division.
- Special Crime and Counter Terrorism Division; and
- Specialist Fraud Division.

In addition, the CPS Proceeds of Crime is a dedicated division responsible for all restraint, enforcement, and serious confiscation work.

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

2.2 Our values

1. We will be independent and fair
2. We will prosecute independently, without bias and will seek; to deliver justice in every case.
3. We will be honest and open
4. We will explain our decisions, set clear standards about the service the public can expect from us and be honest if we make a mistake.
5. We will treat everyone with respect
6. We will respect each other, our colleagues and the public we serve, recognising that there are people behind every case.
7. We will behave professionally and strive for excellence
8. We will work as one team, always seeking new and better ways to deliver the best possible service for the public. We will be efficient and responsible with taxpayers' money.

2.3 Equality and inclusion

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

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

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

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

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

2.4 Why Work with CPS

Impacting on Criminal Justice: The CPS is responsible for delivering justice through the independent and effective prosecution of crime, as the principal prosecuting authority across England and Wales. We have a clear mission to make sure that the right person is prosecuted for the right offence, and to bring offenders to justice wherever possible. Working as supplier for CPS opens opportunities for your organisation to play a key role in achieving these outcomes and enhancing the service we provide to victims and witnesses of crime.

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

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

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

Committed to breaking boundaries: The CPS is heavily invested in developing our digital capability as an integral part of our CPS 2025 Strategy. We have launched exciting initiatives aimed at increasing our use of innovation and developing the casework tools that we will use in the future; are committed to delivering new core ICT, and to securing our data and

unlocking its value. Working as a supplier for CPS opens opportunities for your organisation to be at the leading edge of this preparation for our future.

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

2.5 The ICT Environment

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

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

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

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

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

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

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

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

3 Contract Scope

The CPS is seeking to procure a Service Desk service that will be the first point of contact for all ICT related issues to:

a. CPS end users
b. The Attorney Generals' Office,
c. HMCPSI
d. Some Police staff who use the Witness Management System

The Supplier will use the CPS's IT Service Management (ITSM) tool ServiceNow in its current configuration to provide a service desk to the CPS, as well as to provide a service allowing other suppliers in the CPS supply chain to provide updates on incidents and requests. Access to ServiceNow and licenses will be provided by the CPS.

The CPS's key hours of operation are 7am to 7pm. However, there are a limited number of business-critical functions that operate 24 x 7 and have teams working on a 24 x 7 basis.

The service desk currently handles approximately 10,000 tickets a month which are a split of approximately 50% incident tickets and 50% service requests. The Buyer requires a supplier with appropriate experience of working collaboratively within a multi supplier environment.

In addition to the Service Desk Supplier, the key suppliers of services within the Buyer ICT environment are currently:

- Network Services Supplier
- Applications and Hosting Supplier
- End User Device Supplier
- Modern Workplace – End User Compute support, including Office 365 and Oracle and in-house applications. (internal provision)
- Print Services Supplier

Both internal teams and external suppliers act as resolver groups in ServiceNow to manage the services. There are also other external suppliers who provide applications used for business critical services, which are supported on a 24 x 7 basis.

3.1 Service Desk Vision & Scope

The Service desk is a key tool for enabling CPS employees to carry out their role effectively.

CPS requires the Service Desk to be at the forefront of taking the pulse of the daily needs of the user community, responding quickly when there is a new issue and for example identifying when a knowledge article is needed or where a response to a security issue is required.

The overall goal is to systematically and actively reduce the need to call the service desk i.e. to follow a continuous improvement cycle of identifying root cause, removing the problem and this then leading to a reduction in the call numbers.

As stated over half of our contacts are for request fulfilment and we are looking for that to be an efficient process, using self-service and automation where possible. We are on the start of this journey in Service Now and would value a Service Desk partner to bring tried and tested approaches to our attention and then to deliver those savings.

When issues arise and there are problems with the IT systems, we are looking for the Service Desk managers to alert to our Service Management team on the real-time trends to allow for real-time interventions. The Service Desk supplier will lead on managing our Problem and Major Incidents, drawing on our internal and external suppliers to effect resolutions via a consistent triage process.

We seek a Service Desk partner to work with us and our eco system of suppliers to minimise the need to use the Service desk, but where the need remains, its Accessible by Default.

We are looking for a supplier who can manage a service desk, using skilled operatives on the line and digitally, and can support us in adopting innovative and accessible mechanisms to reward their contribution. We have ambitious goals for reducing the need to call the service desk in the next 5 years.

The scope of the service desk is broadly as set out in the table below:

1	Act as a single point of contact (SPOC) for Users seeking assistance relating to any of the Buyer's ICT services. The Service Desk will log tickets consistently and assign an agreed priority. The Service Desk will manage all Incidents through to resolution and support Users who report known problems. The Service Desk will co-ordinate with the Other Suppliers to ensure normal service is resumed as quickly as possible and within agreed service levels e.g. resolving of an Incident, fulfilling Service Requests and responding to enquiries.
2	The Supplier will be provided with access at appropriate levels to the Buyer's provided ITSM (Service NOW), which will also be accessed and updated by the Buyer and Other Supplier support teams. The Buyer's ITSM will be used by the Supplier to manage the following processes and all functions will be recorded in the ITSM. • Incident Management • Major Incident Management • Problem Management

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

3.2 Current Infrastructure and Applications

3.2.1 Infrastructure

Modern cloud-managed Microsoft Surface laptops allow our users to connect to our corporate applications remotely or from the office. The majority of our applications are public cloud based. The key core applications of Case Management (CMS), Witness Management (WMS) and its Management Information Service (MIS) are hosted in two secure datacentres.
All offices and some courts are provided with cloud managed Multifunction devices (MFDs) as part of overall managed Print service including Bulk Print and Bulk Scan offerings. The MFDs are capable of providing printing, copying and scanning to email services.

The core Applications include:

a. Windows 10 operating system (current aim is to move to Windows 11 during 2024)
b. Microsoft Office 365 (Word, Excel, PowerPoint, Access).
c. Microsoft Outlook
d. Edge Chromium internet browser
e. Adobe Acrobat Reader and Professional software (for viewing PDF documents)
f. VLC player (to support viewing multimedia evidential material)
g. These currently run on Windows 10 operating system (current aim is to move to Windows 11 during 2024)

Further Applications may be added to the core Application before Call Off Contract award.

3.2.2 Buyer Corporate Applications

a. Case Management and Witness Management System (CMS/WMS)

The CMS is a national Case Tracking and Management System which provides case management for criminal cases. There are approximately 6,000 users of CMS.

CMS is a centralised application which is hosted by the Applications Support 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. Due to legacy browser dependencies, this application is using IE mode in Microsoft Edge Chromium internet browser.

WMS holds all relevant information on witnesses and shares the same back-end database as CMS. WMS is used by the CPS as well as the police forces across the UK.

b. Prosecutor Application

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

c. Management Information System (MIS)

Associated with CMS/WMS is a management information system (MIS) that provides statistical and summary information on the progress of cases.

d. Intranet

The Buyer intranet service is hosted on Share Point which resides on Azure. It is accessible to all Buyer staff via the Buyer Network.

3.2.3 Assistive Technologies

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

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

4 General Requirements

#	Requirement
G1	The Supplier shall answer calls as per the service level agreement. Where possible incidents or requests should be addressed at the first point of contact and where an incident or request cannot be resolved at first point of contact, they are assigned to the right resolver group.
G2	In order for the Buyer to manage the end-to-end service in accordance with their policies and service model, the Supplier and the relevant Other Suppliers are required to adopt the Buyer's integrated set of Service Management Policies and Processes (PPs). This methodology shall drive a common understanding of how all the suppliers shall work collaboratively to deliver service excellence. The suppliers are not required to change their internal Service Management Procedures, only to comply where necessary and adhere to the Buyer's PPs.
G3	The Supplier shall ensure that all processes related to running the service are set out in the Service Operating Manual (SOM).
G4	The Supplier shall ensure that processes related to the production of their Service Level reporting are set out in the Systems of Measurement Reference Document (SMRD). This includes details of the sources of data used, how this data is processed, and what calculations are used in reporting Service Level compliance and Service Credits in the monthly Performance Monitoring Report.
G5	The Supplier shall provide a SOM and a SMRD in accordance with the Implementation plan and update it in consultation with the Buyer each time there is a change to the Supplier's solution. The documents will be baselined annually on each anniversary of the Call Off Commencement Date.
G6	The Supplier shall acknowledge that the Services shall be delivered in a manner which is compliant with the Welsh Language Act 1993 and with the Welsh language scheme that the Buyer is liable to comply with and where required any change required to ensure such compliance shall be subject to the Change Control Procedure. The Supplier shall ensure that it is familiar with the Buyer's current Welsh language scheme which is available at https://www.cps.gov.uk/sites/default/files/documents/publications/CYNLLUN_IAITH_GYMRAEG-WELSH_LANGUAGE_SCHEME.pdf
G7	The Supplier shall comply with the security standards as set out under section 19 "Security" and in the Security Schedule associated with this contract.

G8	The supplier should provide direct contacts for the Buyer's service management team, to ensure the effective operation of this service and agree continuous service improvement activities
G9	The Supplier shall operate to the relevant Digital Accessibility industry standards, including WCAG2.1 AA and customer accessibility standards. Note to Supplier – Please read "Making your service accessible: an introduction" a Service Manual available at GOV.UK (www.gov.uk). The Buyer expects this approach to accessibility to extend to internal facing services as well as public facing services.

5 Availability of the Service Desk

#	Requirement
A1	The Supplier shall ensure availability of the Service Desk 24 hours a day, 7 days a week, including by users with physical and or neurodiverse conditions.
A2	The Supplier shall provide an UK based Service Desk, which will be the initial and single point of contact for all Users to enable them to report problems with any Buyer ICT service, and to request services or assistance. The service desk will respond to users by phone, self-service and other channels. {All Users will be provided with a single Service Desk telephone number for the raising of incidents or queries with the Service Desk. The Buyer will divert this number to the Supplier.}
A3	The Supplier shall, as a minimum, make the Service Desk available to all Users via telephone and through the self-service option on the Buyers ITSM.
A4	The Supplier shall have a call wait time notification on the telephone line, which will inform callers of the likely time to answer.
A5	The Supplier shall ensure that contacts by telephone and other channels are responded to based on the priority levels set out in the Service Levels schedule associated with this contract.
A6	The Supplier shall provide a telephony system for the receipt of calls from Users and Other Suppliers. This telephony system shall be capable of providing appropriate MI reporting regarding all calls received, including but not limited to: a. Volume b. Duration c. Time of Call d. Time to answer e. Abandon Time The supplier shall provide such records in a concise, legible, and easily auditable format. The telephony system should also be capable of recording of calls for quality and training purposes, and the supplier should provide transcription / recording of calls at the request of the customer
A7	The Supplier provided telephony system shall provide a call-back function, so Users can be automatically called back rather than waiting if there is a call queue.
A8	The Supplier's contact number shall be capable of providing IVR and pre-recorded messages, which shall only be implemented after formal authorisation from the Buyers Service Management Team.

#	Requirement
A9	The Supplier shall ensure that any IVR and pre-recorded messages can be updated within 15 minutes following authorisation from the Buyers Service Management Team.
A10	The Supplier shall, where agreed with the Buyer, provide modern voice assistance technologies, in order to support the effective resolution of incidents.
A10	The Supplier shall ensure that it employs an up to date mailing list made up of all CPS users is provided *Note to Supplier – The CPS Service Management function is accountable for timely mass communications regarding service status, however the mailing list is used for such communication.*
A11	Following contact to the Service Desk and after Incident resolution, the Supplier Service Desk shall advise Users of any relevant self-help articles approved by the Buyer.
A12	The Supplier Service Desk shall when appropriate to the type of Incident and its resolution, and with the User's consent, utilise secure remote connectivity and diagnostic tools to resolve Incidents at first point of contact to the Service Desk. The Supplier shall access end user devices using a technical solution provided by the Buyer *Note to Supplier –* *a. The solution will use terminal servers which are hosted in the Buyer's data centres by another supplier.* *b. The Supplier will be provided with training on the solution by the Buyer*
A13	The Supplier Service Desk shall log and pass incidents to suppliers & internal teams, including where necessary to other Criminal Justice System (CJS) agencies as agreed with the Buyer. Such arrangements shall be documented in the SOM.
A14	The Supplier Service Desk shall perform basic management of the CPS ActivCard system (via defined scripts) to provide timely support to Users and deploy ActivID cards on a 24/7 basis. Note to Supplier – It is possible that the Buyer may move away from the ActivCard system either before the award of the ServiceDesk contract or during the contract tenure. In the event this happens, this and other related requirements will be amended under change control.
A15	The Supplier shall wherever possible, try to resolve incidents first time and record their first time fix rate.

#	Requirement
A16	The supplier shall ensure the ITSM records are updated and accurately reflect the position of the incident or service request from the point the record is created.
A17	The Supplier shall on-board and off-board Other Suppliers to the Service Desk function as required and agreed with the Buyer.
A18	The Supplier shall ensure they employ adequate resources to accommodate peaks of effort on the Service Desk
A19	The Supplier shall ensure they recognise Users with Accessibility needs from Standard Users and agree with the Buyer the communication process for each, and the need to manage Users with Accessibility needs in agreement with the Buyers Digital Accessibility team.

6 Incident Management

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

The Buyer's Policy and Process (PP) related to Incident Management has been provided in the data room as part of the Buyer's Service Desk tender documentation.

#	Requirement
I1	The Supplier shall implement Incident logging procedures (which adhere to the Buyer's PPs) with the Buyer and the Other Suppliers during the Implementation phase.
I2	The Supplier's Solution should allow Incidents to be detected (or identified) in a variety of ways, including but not limited to: a. the Event Management process. b. Supplier's or Other Supplier's monitoring activities. c. Availability management processes. d. Capacity Management processes (e.g., events from servers managed by Other Suppliers may result in the registering of an Incident); or e. by the Buyer's technical staff or Users. Irrespective of how an Incident is registered, the Supplier shall record and hold such information to allow subsequent activity to take place to resolve the Incident.
I3	The Supplier shall use the Buyer's Incident management procedures to determine: a. The Incident category and subcategories. b. The priority to be associated with the Incident. c. The resolver group to which the Incident needs to be allocated.
I4	The Supplier shall agree any changes to the Policy or Processes used with the Buyer, prior to implementing any such change.
I5	The Supplier shall accurately record all Incident Management data within the ITSM ServiceNow.
I6	The Supplier shall ensure that each Incident once recorded, is associated with the relevant Service Level within the Buyer's ITSM tool (ServiceNow)
I7	The Supplier shall ensure that each Incident, once recorded, is associated with any existing Known Errors, Problems or other Incident records to support a potential first-time fix or aid escalation to the relevant Resolver Group.

#	Requirement
I8	The Supplier shall assign the required time to fix to the Incident record, and the Supplier shall advise the User of the anticipated fix time.
I9	In the event of a dispute as to the Incident Severity Level assigned, the matter shall be escalated within the Supplier's and the Buyer's organisation
I10	The Supplier shall ensure the ITSM is used to track the elapsed time during the life cycle of the resolution and shall create alerts at predetermined points set out in the SOM. The Supplier shall use this information to monitor the progression of each incident and escalate appropriately with the Resolver Groups.
I11	The Supplier shall use the ITSM so that Incidents are automatically escalated to the Supplier's management at pre-determined points, based on the time that has expired since the occurrence of notification of the incident. The escalation processes shall include procedures for exception reporting to the Buyer.
I12	The Supplier shall validate the User's profile and entitlement to service upon a User recording an Incident at the earliest opportunity.
I13	The Supplier shall own the records for all Incidents and be accountable for their progression throughout the ITIL Incident life cycle.
I14	The Supplier shall provide feedback to Users on progress made with resolving an Incident. Such feedback shall include: (i) advice on any remedial action being taken; (ii) the estimated date and time when the Incident may be resolved; and (iii) advice allowing the User to continue to use the Services until such time as the Incident is resolved.
I15	The Service Desk shall ensure that Incidents are not closed until the User has confirmed that the Incident is resolved. The Supplier shall adhere to the Buyer's PP's with respect to Incident closure and re-opening. The supplier will not close incidents raised by or for Digital Accessibility Users.
I16	The records of all Incidents that cannot be resolved immediately shall be updated with a full description of all triage activity that has been undertaken and then assigned by the Supplier to appropriate specialist Resolver Groups.
I17	The Supplier shall be responsible for managing and progress chasing the relevant Resolver Group(s) to provide a resolution or Workaround.
I18	The Supplier shall pass Incidents to the appropriate Resolver Group, or between Resolver Groups where additional or alternative knowledge is required to resolve the Incident.
I19	The Supplier shall ensure up-to-date self-serve progress reports on any Incident is available to the Buyer and User.

#	Requirement
I20	The updating of Incident data in relation to the Other Suppliers shall occur immediately or in sufficient time to enable effective Management Information to be produced and acted upon in accordance with the Service Levels and the Service Level Performance Measures for the relevant services of the Other Suppliers.
I21	The Supplier shall act as the escalation point for the Other Suppliers for all Incidents that exceed or are expected to exceed their target resolution times.
I22	The Supplier shall be able to identify trends from the Incidents logged and bring this to the attention of the Buyer, as well as act upon them.

7 Major Incident Management

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

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

#	Requirement
M1	All Severity Level 1 and Severity Level 2 Incidents shall be defined as Major Incidents. The Supplier's Solution shall provide a 24 x 7 Major Incident Management Team to provide focussed Major Incident Management across all Suppliers in accordance with the Buyer's Policies and Process documents (PPs)
M2	The Supplier shall ensure that the Major Incident Management Team is engaged as soon as Incident prioritisation determines that the conditions for a Major Incident are met.
M3	The Major Incident Management Team shall co-ordinate the efforts of the Service Desk, as well as resources required from Other Suppliers, during the life cycle of the Major Incident.
M4	The Major Incident Management Team shall keep the nominated Buyer Representative updated on an hourly basis of progress made with resolving the Major Incident (unless otherwise agreed by the Buyer) and cascade to Other Suppliers (as agreed by the Buyer).

#	Requirement
	The format of the updates shall be agreed during implementation.
M5	The Major Incident management Team will operate 24/7 and in the event of a Major Incident, will coordinate resources from across the supplier eco-system as required to ensure major incidents are resolved within the assigned service levels.
M6	The Major Incident Management Team shall ensure that relevant Resolver Groups provide a detailed breakdown of the Incident to the Major Incident Management Team, along with details of any remedial actions that have been conducted, any that would be recommended/require approval from business stakeholders, and any works planned.
M7	The Supplier shall provide an initial point of contact for the Buyer Service Management Team for escalation and information purposes during the lifecycle of the Major Incident.
M8	Once the details of the Major Incident have been explained, the Major Incident Management Team shall decide whether to direct additional technical resources to work on the Incident or continue with the existing resource levels.
M9	The Supplier shall, create a Major Incident check list to be set out in the SOM. This check list to contain the generic steps needed to progress and report on a Major Incident. The check list to be approved by the Buyer as part of Implementation and maintained by the Supplier throughout the Term.
M10	Upon an Incident being classified as a Major Incident, the Supplier shall create a Major Incident check list specific to the Incident and progress the Major Incident until resolved using the check list.
M11	Upon an Incident being classified as a Major Incident, the Supplier shall perform the following actions immediately: a. Assign a lead to the Major Incident Management Team; b. Advise the relevant Resolver Group lead that a Major Incident has been identified and allocated to the Major Incident Management Team for investigation and diagnosis; c. Inform the Supplier's Major Incident manager (or deputy)(if not already informed); d. The Supplier's Major Incident manager shall liaise with the relevant Resolver Group(s) for an initial Major Incident status update including estimated resolution delivery timescale; e. The Supplier Major Incident manager shall update the contact points (as defined in the Buyer's Incident Management Policy) with the current Major Incident status; f. The Supplier's Major Incident manager shall update the Major Incident record with ongoing status; g. The Supplier shall consider recommending to the Buyer that a telephone message or other contact channel is added advising Users of an ongoing Major Incident to

#	Requirement
	the Interactive Voice Response (IVR) system; h. The Supplier's Major Incident manager shall update the Major Incident checklist; i. The Supplier's Major Incident manager shall liaise with all relevant parties using the defined contact channel at each stage of the process.
M12	The Supplier shall ensure that appropriate input from Other Suppliers is provided to the Major Incident Management Team where required until the Incident is Resolved.
M13	If the relevant input is not provided by the Other Suppliers, or the Incident is not progressing appropriately to meet the applicable Service Levels or resolution process, then the Major Incident Management Team shall escalate the situation to the Buyer Service Management incident lead immediately.
M14	When the Major Incident fails (or at the point it becomes clear that it is in danger of failing) it's applicable Service Level, the Supplier's Major Incident Management Team shall immediately call an all party Major Incident progress call to agree actions required.
M15	The Supplier shall ensure that the Major Incident Management Team progress call has appropriate representation including resources from Other Suppliers and the Buyer Service Management Team where required.
M16	The Supplier shall ensure that the Major Incident Management Team progress calls are maintained at regular intervals until the Incident is Resolved.
M17	The Major Incident Management Team shall produce, through discussion on the calls, a plan detailing the remedial actions to be taken and communications required by whom.
M18	The Major Incident Management Team will nominate a team member to advise the nominated Buyer Representative of the action plan and expected timescale until the Incident is Resolved.
M19	The Supplier shall ensure that a Major Incident Exception Report is produced and issued for all Major Incidents which have failed their applicable Service Levels. Ensuring appropriate input from the Other Suppliers and including details such as, but not limited to: • Date/Time • Duration • Category • Service affected • Business impact • Incident description • Incident summary and actions performed • Incident event timeline • Resolution and results of root cause analysis • Recommendation whether a Problem Investigation is required

#	Requirement
	• Recommended actions to prevent recurrence The format of the Major Incident Exception Report and process for issue shall be agreed with the Buyer during the Implementation Period.

8 Problem Management

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

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

	Requirement
P1	The Supplier shall work with the Buyer and Other Suppliers to define and implement the criteria for prioritisation of Problems.
P2	The Supplier shall maintain Problem Management records using ServiceNow.
P3	The Supplier shall ensure that Problem records contain the following details as a minimum: a. Date and time of Problem raised b. Relevant dates and times of occurrence of any Incidents c. Category d. Business impact/urgency e. Resultant priority f. Actions taken/history/timings g. Links to resultant Incidents h. Name of person who made the modification i. Date and time of modification j. What the person modified (e.g. priority, status, history) k. Why they made the change l. Next actions and timescales m. Details of any interaction with the Buyer n. Links to relevant knowledge management articles o. Supplier who owns the problem investigation.
P4	The Supplier shall ensure that Problem Investigation is carried out typically for: a. Incidents for which the root cause is unknown b. All Major Incidents c. For Incidents which have been repeated or where there are indications that they are likely to be repeated.

	Requirement
P5	The Supplier shall retain overall responsibility for recording and tracking Problems until the Problem is closed.
P6	The Supplier shall allocate Problems to Other Suppliers or a Resolver Group as appropriate.
P7	The Supplier shall progress all activities required to diagnose the root cause of Major Incidents and Problems and to determine their resolution.
P8	On the Buyer's reasonable request, the Supplier shall undertake all activities required to diagnose the root cause of all problems and to determine their resolution.
P9	The Supplier shall co-ordinate the effective execution of Problem investigation and diagnosis across Other Suppliers to identify the fault in the Service that caused the Problem.
P10	The Supplier shall recommend to the Buyer measures to prevent the recurrence of all Problems.
P11	The Supplier shall initiate action to negate or eradicate where possible the root cause of all Problems, such actions to be agreed with the Buyer.
P12	The Supplier shall record Known Errors and their Workarounds or Problem resolutions in the ITSM.
P13	The Supplier shall conduct Problem Management meetings as required by the Buyer, to prioritise the resolution of Problems.
P14	The Supplier shall maintain regular communications between all relevant parties until Problem resolution is achieved.
P15	The Supplier shall escalate to appropriate management within any Other Supplier's organisation structure if corrective actions are not being progressed.
P16	The Supplier shall document and publish Problem Management meetings status reports to the Buyer and to Other Suppliers.
P17	The Supplier shall receive Problem Management information on a monthly basis from Suppliers and produce trend analysis and management summaries to identify trends, significant changes or increases in Problem volumes for discussion with the Buyer and Suppliers at the appropriate forums.

9 Change Management

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

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

#	Requirement
C1	The Supplier shall adhere to Buyer PPs. and, where requested, contribute effort to requests which require Changes across the Multi-Supplier Operational Environment. The supplier will create and provide new scripts if/when new suppliers are onboarded. These scripts will be stored in the customers ITSM tool.
C2	The Supplier shall take all such actions as required to enable the Buyer to respond to urgent requirements for Change, as set out in Call Off Schedule 5 (Change Control Procedure) and in the Change process Policies and Processes (PPs).
C3	The Supplier shall provide the flexibility to "fast track" certain Changes, where urgent requirements for Change have been identified by the Buyer. Call Off Schedule 5 (Change Control Procedure) articulates the process for handling such Change.

10 Operation of a Service Desk

#	Requirement
OSD1	The Supplier shall ensure all components that make up the Services (e.g., Service Desk) continue to be of sufficient capacity to meet the Buyer's operational needs. This includes providing sufficient capacity to cater for growth in use over the Call Off Contract Period.
OSD2	The Supplier shall provide a dedicated Service Desk Management team to oversee the operation of the services, and ensure that all services are delivered in line with the contract and the Buyers expectations.

11 Service Asset and Configuration Management

Service Asset and Configuration Management aims to maintain information about Configuration Items (CIs) required to deliver an IT service, including their relationships

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

12 Request fulfilment management

ITIL Request Fulfilment aims to fulfil Service Requests, which in most cases are minor (standard) Changes

#	Requirement
R1	The Supplier shall manage the Buyer's Business Service Catalogue in accordance with the Buyer Policy and Process documentation relevant to Service Requests management.

#	Requirement
R2	The Supplier shall review management reporting information on a monthly basis to identify trends or significant changes or increases in Service Request volumes, for discussion with the Buyer and, where necessary, Other Suppliers.
R3	The Supplier shall identify possible process improvements and promptly make appropriate recommendations to the Buyer.
R4	The Supplier shall ensure that all information relevant to a Service Request is promptly provided by the Supplier to the Service Desk in response to Service Requests.
R5	The Supplier shall proactively manage and monitor the status and progress of fulfilling Service Requests.
R6	The Supplier shall respond to the Buyer's enquiries regarding Service Requests with accurate and up-to date information

13 Event Management

Event Management, as defined by ITIL, is the process that monitors all events that occur through the IT infrastructure. It allows for normal operation and also detects and escalates exception conditions.

An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.

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

14 Access Management

Access Management aims to grant authorized users the right to use a service, while preventing access to non-authorized users

#	Requirement
AC1	The Supplier shall validate the identity of a User and their right to access the Buyer ICT Environment by using the Buyer's security database held within ServiceNow.
AC2	The Supplier shall, for all IT Services, where they have the capability and authorisation to do so, reset passwords for Users on request. They shall do this after validating the identity of the User using the ServiceNow password recovery database, and their right to access the requested services.
AC3	The Supplier's Solution shall ensure an automated process whereby the User receives a follow up [accessible] e-mail after a password is reset.
AC4	The Supplier shall reject any request that has not been properly approved in accordance with the Buyer's Access Management Policy and notify the customer accordingly.

15 Knowledge Management

ITIL Knowledge Management aims to gather, analyse, store and share knowledge and information within an organization. The primary purpose of this ITIL process is to improve efficiency by reducing the need to rediscover knowledge

#	Requirement
K1	The Supplier shall capture details of Known Errors as soon as they are known and record it in the ITSM.
K2	The Supplier shall store Service Desk scripts in the ITSM, such that similar responses are provided for similar Incidents.
K3	The Supplier shall support the Buyer in the identification of Knowledge Articles that can help users find self-help to common issues.

16 Continual Service Improvement

The *Continual Service Improvement (CSI)* process uses methods from quality management in order to learn from past successes and failures. The ITIL CSI lifecycle stage aims to continually improve the effectiveness and efficiency of IT processes and services, in line with the concept of continual improvement adopted in ISO 20000.

#	Requirement
CS1	The Supplier shall review all of the Services on a regular basis, with a view to improving service quality and accessibility where necessary, and to identify more effective and efficient ways of providing the Services where possible.
CS2	The Supplier shall evaluate processes on a regular basis. Such evaluation to include identifying areas where Service Levels are not reached, holding regular bench markings, audits, maturity assessments and reviews.
CS3	The Supplier shall define specific initiatives aimed at improving services and processes, based on the results of service reviews and process evaluations. The resulting initiatives shall either be internal initiatives pursued by the Supplier on its own behalf, or initiatives which require the Buyer's cooperation. Any such initiatives will require the approval of the relevant role within the Buyer's Service Management Team.

#	Requirement
	Note to Supplier - Roles and responsibilities will be agreed as part of the Supplier on-boarding process.
CS4	The Supplier shall verify if improvement initiatives are proceeding according to plan and introduce corrective measures where necessary.
CS5	The Supplier shall foster a culture which allows Supplier Personnel to capture, prioritise and communicate ideas across their teams, allowing any Supplier Personnel to suggest innovative and accessible improvements.
CS6	The Supplier shall provide training, share best practice and enhance the knowledge of the end users on the IT service provided.

17 Service Level monitoring and MI reporting

The Buyer requires access to regular reports that cover performance reporting, that is not limited to the Service Levels monitored as part of the service.

#	Requirement
SL1	The Supplier shall monitor Achieved Service Levels and compare them with agreed Service Level Performance Measures. This information shall be used as a basis for measures to improve service quality.
SL2	The Supplier will provide Service Performance Monitoring Reports that compare the Service Levels with the Achieved Service Levels, and include information on the usage of Services, ongoing measures for improvement of the Services, and any exceptional events that occurred during the period measured.
SL3	The Supplier will produce reports (when information is not available via the MI reporting tool) to be provided to the Buyer within agreed timescales to be set out in the Systems of Measurement Reference Document (SMRD)
SL4	The Supplier shall use the ITSM to capture sufficient details to allow data to be extracted for the purpose of assisting in production of Service Management Reports for: (1) the Supplier's reporting against its Service Levels under this Call Off Contract. This should be presented in a legible format that is auditable. The data and reports shall be agreed during Implementation and shall include, but not be limited to: a. Details surrounding Incidents where the resolution of such Incidents has exceeded the Service Level Target relevant to the Incident Category assigned to the Incident.

#	Requirement
	b. Where the failure to resolve an Incident within the Service Level Target relevant to the Incident, is a Repeat Failure, a progress report on the actions taken by, or on behalf of, the Supplier to Resolve the underlying cause and prevent recurrence. c. which Incidents have been Resolved and their Incident Resolution Times. d. which Incidents remain outstanding and the relevant Supplier's progress in Resolving them. e. reporting on aged Incidents
SL5	The Supplier shall ensure the data captured via the ITSM is timely and accurate such that other suppliers' reports relying on such data, accurately reflect the position at the end of the month.
SL6	The Supplier shall provide reports and data on trends and root cause analysis to: A. allow the Buyer to make informed decisions. B. allow for pro-active management of issues
SL7	The Supplier will provide, within their monthly performance report, reports with analysis to show: • Aged ticket analysis • Trending of Availability and Service Credits for the past six months • Call quality trending over the past six months (abandoned calls/abandoned calls over 20s/average queue times • First Time Fix trending over the past six months (Incidents) • Trending of Incident and Request volumes over the past six months including logged/resolved/cancelled/re-opened/carried forwards • Trending of incidents logged by severity level over six months • Top 10 incident types for the Service Period • Top 10 request types by template for the Service Period • Top 10 self service request types for the Service Period • Top 10 types of re-opened incidents for the Service Period • Trending of tickets by channel over the past six months • Trending of password re-sets by type over the past six months • Change Management – changes completed and Impact Assessments submitted in the reporting period • Forward view of change for following reporting period • Breakdown of Problems opened/closed/active in the reporting period. Additional table showing detail of active problems showing number of days to root cause identification/comments on reason for any delays • Trending of any customer satisfaction survey outcomes • Table of active Continuous Service Improvements/Risks/Issues

#	Requirement
	And any additional reports agreed with the Buyer.

18 Customer Satisfaction, surveys and complaints

#	Requirement
CSS1	The Supplier shall support the Buyer in identifying and implementing methods of assessing customer satisfaction across all the services in the Buyer ICT Environment.
CSS2	The Supplier shall support the Buyer in reviewing customer satisfaction results across all the services in the Buyer ICT Environment.
CSS3	The Supplier shall, as a minimum, utilise their experience and expertise to recommend improvement actions required to increase customer satisfaction rates.
CSS4	The Supplier Service Desk shall issue accessible Customer Satisfaction Surveys, as agreed with the Buyer.
CSS5	The Supplier shall implement processes to maintain the quality-of-Service Desk performance in accordance with Service Levels and to address identified customer satisfaction issues (such as survey results and complaints).
CSS6	Service Desk Analysts will be consistently managed and monitored by the Supplier, so any training issues are addressed by the Supplier (including technical and behavioural).
CSS7	The supplier shall participate in collating relevant information and producing written responses to the Buyer in respect of customer complaint

19 Security

#	**Requirement**
SE1	Supplier Personnel shall be subject to pre-employment checks and will ensure compliance with security clearance requirements prior to deployment of any staff onto the CPS account, as outlined in the security schedule. Supplier personnel should ensure prompt notification of any change in personal circumstances, or when an employee has left, or moved away from CPS work and no longer requires a security clearance. Change employee circumstances or new information obtained about employees which could have an impact on security clearance or suitability to operate in their role accessing the organisations systems should be reported to the organisation (e.g. arrest/convictions etc) in a manner that's in accordance with data protection laws and regulations.
SE2	The supplier shall have in place an appropriate disaster recovery policy and process, including secure backup solutions, to maintain continuity and minimise downtime/impact to the CPS in the event of an incident at the supplier side.
SE3	The supplier should be able to evidence the security of their network where any such systems access CPS systems and data, or store CPS data.
SE4	The Supplier shall ensure that the system is governed to NCSC standards but must provide audit data to comply with, or facilitate compliance with, the applicable requirements of the NCSC's Minimum Cyber Security Standard - GOV.UK (www.gov.uk). All accounting data shall be exported automatically by a standard method and held for a timeframe in line with agreed compliance and legislation. As a minimum the Supplier will need to be ISO27001 certified, and Cyber Essentials Plus accredited.
SE5	The Supplier shall provide the Buyer access to Supplier Staff and Supplier premises as required for the purposes of improving and auditing security. The Supplier shall make available to the Buyer and its designated agents any reasonably requested resources including physical access to the Site, facilities and Key Personnel that support the delivery of the Service Desk requirement.
SE6	If any equipment or systems fall outside the scope of the buyer estate, then the Supplier shall be responsible for the required IT HealthChecks/Penetration Testing to the satisfaction of the Buyer on an annual basis. All IT HealthCheck / Penetration Testing shall be delivered by a NCSC approved penetration testing service provider.
SE7	The Supplier shall ensure that access to all Service interfaces is limited to authenticated and authorised Service Desk Administrators & Users only with appropriated auditing mechanisms in place. These reports should be made available to the buyer upon request.

SE8	The Supplier shall deploy an effective authentication process for any devices to the network services they access which should include the following aspects: • User to device, whereby the User shall only be granted access to the device following successful authentication to the device; • User to service, whereby the User shall only be able to access services after successful authentication to the service via their device; • Device to service, whereby devices are only granted access following successful authentication to the application environment.
SE9	The Supplier shall deploy an 'incident response' arrangement that aligns with wider response procedures in place across the Buyer ICT Environment.
SE10	The supplier would be expected to deliver a Security Management Plan in line with the services delivered by the supplier as part of the contractual agreement. This should be reviewed annually by supplier & buyer and mutually agreed.

20 Digital Accessibility Compliance

#	Requirement
DA1	The supplier shall ensure all aspects and elements of services meet the Web Content Accessibility Guidelines (WCAG) 2.1 AA as a minimum, at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA2	The supplier shall ensure all aspects and elements of services meet the customers compliance auditing standards, at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA3	All training and communications provided by the supplier must meet WCAG 2.1 AA as a minimum, and the customer's compliance auditing standards, at all times. Any exclusions must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA4	Any workarounds to meet WCAG 2.1 AA and or compliance auditing standards, must be agreed by the Buyer's Digital Accessibility Compliance Team.
DA5	Any workarounds to meet WCAG 2.1 AA and or compliance auditing standards, must have a resolution plan agreed by the Buyer's Digital Accessibility Compliance Team, and be implemented at the pace agreed.
DA6	The Supplier shall triage and direct contacts from Digital Accessibility users to the resolver teams as directed by the Buyer's Digital Accessibility Compliance Team.
DA7	The supplier shall provide an accessibility statement before any type of go-live, including transition, launch, change and be reviewed at least annually.