CRFCA Managed Service Provider - Service Catalogue (ITT Appendix C, part 1)

SERIAL	SERVICE	SUB SERVICE	SERVICE DESCRIPTION
	PH2 MSP		
1	Software Development		Software development service is provided as per project requirements or in support of the MSP business.A wide range of software development skills are needed to support the current custom applications. This includes ORACLE DB, ORACLE Apex, PL SQL, SQL Scripts, C#, PHP, Dot Net, HTML, JAVA. The PH2 Contract requires software development support for in house development and to maintain the current applications in the sub list below
2		PQQ	PQQ is an ORACLE APEX Application, supporting the RFCAs need to manage their contractors through a Pre Qualifications Questionaire prior to engaging with them for estates management business. The PQQ is assessed by the Estates and Finance departments to approve the PQQ of a contractor, the contractor's details are sent to Symphony using XML file. See Symphony in Third Party Applications for more details.
3		CASTRA	Castra is an application that enables sharing of sensitive data between the RFCAs Estates departments and their contractors. The Castra System is responsible for communications and management of the data, the legal contracts are agreed and issued by the RFCAs prior to utilising this system to manage the actual contracted tasks.
4		User Access Control	User Account Control (UAC) is a web based application hosted in PH2E, but accessible from only within the PH2 and PH2E Intranet. This application contains the following modules and each one of them is explained in detail in this section: Asset Management, User Accounts Management, Asset Management, User SyOPs Control, RSA SyOPs Control
5		Alternative Venues	The aim of the public site (www.alternativevenues.org) is to provide information to the general public about the venues and their facilities available to rent for various occasions. Alternative Venues initiative is aimed to have the same look-and-feel across all regions, but at the same time giving the flexibility for the regional variations and to advertise the regional venues. This is achieved by having a central landing page with menu options that takes the visitors to the regional portals. The
6		Constructionline	Constructionline is a Warburg Pincus owned business (taken over from Capita in Jun 2018) that allows the contractors to register with them for a fee to maintain their company and insurance details. Constructionline vets the data submitted by the contractors and takes the onus away from the buyer organisations such as the RFCAs who are able to subscribe for a fee and obtain the details of these contractors. The software development by the MSP involves designing and managing the data flow from construcitonline, into the PQQ above and exporting it to Symphony (See third party applications) There is a need to validate the accuracy of data and protect against any security risk to Symphony.

7		Intranet Portal	Maintain a set of web pages, published in dot net and SharePoint for providing various links and user level information.
8		Asset Management	User Account Control (UAC) is a web based application hosted in PH2E, but accessible from only within the PH2 and PH2E Intranet. This application contains the following modules and each one of them is explained in detail in this section: Asset Management, User Accounts Management, Asset Management, User SyOPs Control, RSA SyOPs Control
9		RFCA Business Portal	RFCA Commercial Portal is built using 2 different technologies; the public site is developed using a Content Management System (CMS) called DotNetNuke (DNN) and the secure site (for Contractors and RFCA Staff) is built using Oracle Application Express (APEX).
10		RFCA Cloud	RFCA Cloud is a file sharing portal hosted within PH2E infrastructure and accessible via public url, anywhere in the world. The users of PH2 / PH2E are able to share the files between themselves or with external agencies. The sharing could be a bidirectional depending on what the user wants to do.
11	PH2 Catalogue Service		Provide the customer with a list of approved items that have been tested as per the customer's requirements. The cost is agreed in advance and the specifications are fixed until a change is authorised. There must be ready stock to meet the demand within an agreed period, which can be a matter of days rather than weeks. These products are made available on the catalogue purchase website, where the customer with pre-agreed credit is able to order for next day or 48 Hour delivery in most cases.
12		Hardware	The desktops, laptops and tables are supplied as per the customer's specifications and the software build of the operating system and the authorised applications are installed and configured prior to dispatch.
13		Software	A pre tested and approved list of software is available for the customer to purchase from the catalouge website. This software is tested by SPOC against unauthorised data leak or any other security risk. The software requirements are specified by the customer.
14		Peripherals	Pre-agreed list of peripherals are made available for purchase on the catalogue website.
15		Credit Management	Customer is offered a 30 day net terms for all purchases as default, however longer term credit limit is agreed as necessary. The customer is invoiced on the day the goods are dispatched.
16		Stock Management	The product catalogue agreement assures the customer that the tested and agreed standards of hardware and software can be maintained for a long period. This is normally a minimum of 12 months, and maximum of 3 years. Failure to do this would introduce a large variations of hardware, software, that requires greater testing and higher cost of system maintenance.
17		Product Testing	Each product in the catalogue is tested against the customer's statement of need and security standards.
18		Product Selection	The selection of products for the catalogue are agreed after understanding the customer's needs, technical specifications, and costs have been accepted by the customer.
19		Statement of Need Review	SPOC assists the customer in reqviewing the statement of need against technical specifications and availability of funds.

20	Professional Services		A range of professional services are available to the customer that can be called on as the need arrises. The cost of these services is pre-agreed and a bundle of Engineering/Consultancy days are pre-authorised. This service is in support of maintaining the systems at the appropriate security/accreditation level.
21		Systems Architect	The System Architect is responsible for the complete system design and ensuring it meets the user, security and legal compliances.
22		Project Management	Project Management service is available for the customer to call on. This can be software, hardware or other CIS related project. Prince2 qualification is not always necessary but an appropriately qualified/experienced staff are made available to meet the requirements.
23		Change Implementation	SPOC is able to manage any change to the CIS system, the need for this service would be agreed as part of Request for Change review.
24		DPO Support	To provide any technical, procedural, documentation, or data related support to the customer's Data Protection Officer. This could be related to Accreditation, GDPR, FOI, Audit, MOD Policies etc.
25		General Consultancy	Provide the customer with consultancy of the appropriate type/level to address the identified requirement.
26		Design Consultancy	Provide consultancy to draft and agree the design for any CIS related tasks. This could be, hardware, software, processes, change, customisation, re-location etc
27		Security Assurance Co-Ordinator Service	Provide the service of a SAC to meet the system accreditation and ongoing liaison with the authorities.
28		Policies Draft	Provide appropriately skilled staff to assist in drafting any policies or similar documents.
29		Policies Review	Provide appropriately skilled staff to assist in Reviewing any policies or similar documents.
30		ISMB Support	Provide a senior representation at the customer's ISMB and any supporting documents
31		MISB Support	Provide a senior representation at the customer's MISB any supporting documents
32	Telecom Service		Provide a secure VOIP Enterprise Telecome system using the AVAYA systems framework. Integrate with the customer's IT systems and enable user devices to be used as part of the VOIP and VTC solution. The solution must be maintained by SPOC and utalise existing internet connectivity where possible.
33		PSTN Service & Support	Manage connections and rules for connecting the corporate system to the external PSTN, including limitations of numbers, international calls, primary numbers.
34		VOIP Systems Design & Installation	Carry out a survey to assess the customer's requirements, including migration of existing numbers and availability of the necessary services and space requirements.
35		Systems Migration	Where possible, the old numbers are migrated to the VOIP system and a detailed plan for the switchover day is agreed with the customer. Causing minimum distruption to the telephony service.
36		Analogue Device Support	The telecom system is able to integrate any PSTN device, such as Fax, Franking machine and door security system
37		Telcom Maintenance & User Support	Maintain the system with regular updates and provide user support, including use of the system in an integrated environment, using outlook and Avaya Client.

38		Video Conf Support	Configuration and management of the VOIP system's integration with Skype For Business Video Conf calls.
39		Skype for Business Integration	Configuration and management of the VOIP system's integration with Skype For Business, including VOIP calls made from Skype of the Avaya Client.
40	Third Party Suppliers Support		Provide the appropriate level of assistance to the customer to manage the third party suppliers, providing service into the managed system.
41		MOD	Assist the customer with their relationship with the MOD and during the MOD's physical and procedural inspections.
42		External Contractors	Assist the customer with any CIS or policy related issues with the third party's use of the system. This could be trouble shooting communications or data issues as well as providing consultancy to review the third party contracts.
43	Software Licensing Management		SPOC maintains list of software used on the system, irrelevant of how it is licenced.
44		CRFCA Managed	Software funded by CRFCA, as per system requirements
45		RFCA Managed	Software purchased or funded by the RFCAs
46		MSP Managed	Software funded and purchased by the MSP for system management
47	SCIDA Liaison		Work with the SCIDA authority and liaise all SCIDA tasks for the supported system
48		Review SCIDA ECRs	Review the ECRs issued by SCIDA and assist the RFCAs in implementing the changes
49		Third Party Contractors Liaison	Assist the RFCAs in obtaining quotes for the rectification work and review them for cost and compliance
50		SCIDA Authority Inspections Liaison	Liaise with SCIDA for site visits
51		Networks Design Support	Assist SCIDA and the RFCAs in establishing the required design to meet the SCIDA observations and meet the MOD standards
52	Change Management		Assist the customer in establishing the change management boards and helping to run them. Assist the customer in establishing the appropriate Terms of Reference for the CAB and ECAB, in line with ITIL recommendations.
53		CAB	Collect the Request for Change (RFC) and process them for impact assessment and solution to the required change. Present the RFCs to the CAB, talk them through, including costs. The CAB is chaired by the customer and supported by SPOC as required. The Scheduling of approved RFCs is done by SPOC. CAB meets once each quarter.
54		ECAB	Communicate the change to ECAB by the approved method, and act on the agreement obtained. Ensure that ECAB is provided with the correct information and within reasonable time for the decision to be agreed. The decision to communicate the change to ECAB must rest with the senior customer. ECAB agreement can be obtained without a physical meeting being held. ECAB can be invoked at any time the need arrises.
55	RFCA/ACF On Sites Support		The MSP is responsible for managing the system devices, physically, configuration and maintenance. There is one server, firewall, switch and internet SDP equipment at each site, which SPOC has full control over. However, the physical management of these devices and the physical LAN set up is the responsiblity of each RFCA/ACF.

56		RFCA Funded Tasks	Change that requires the equipment to be moved. Upgrade to the cabinet or WAN communications. LAN upgrade to meet SCIDA requirements. Sharing the WAN Connection. Installation of WiFi Service, could all be funded by the RFCA. The authority for change must be obtained through CAB.
57		CRFCA Funded Tasks	Change/upgrade to the infrastructure equipment, including , Server, Firewall,Switch.
58		MSP Tasks	Warranty issues, maintenance tasks that migth require site visits.
59	R&D		Research and Development (R&D) is carried out when required for a new solution or in support of an RFC. This can involve hardware, software or change in configuration to meet the requirements.
60		Funded R&D	RFCs and new solutions are funded R&Ds
61		Unfunded R&D	Problem resolutions or changes brough about by the MSP contracted tasks are unfunded R&D actions.
62	Secure WiFi Service		Managed Wi-Fi provide the PH2 users and guest the ability to be able to connect to an accredited WiFi system, which is available at their normal place of work and the same account is authorised for WiFi connection at any other site served by the PH2 WiFi system. This allows the CRFCA to manage an organizational WiFi network centrally with enhancement of high level of security and enforce company-specific acceptable usage policies. The WiFi system does not connect the user to the trusted (production) networks, the user still has to use the PH2 VPN, if they wish to access the PH2 applications. The WiFi system is routed through the local firewall, on a separate port than the trusted network. It is routed as below and the traffic is not permitted to go over any of the Intranet ports.
63		Infra Set up	The RFCAs request the service and SPOC is reponsible for the design of the Infra at each site. Once the design and funding is authorised, SPOC is responsible for the physical installation and configuration of this service. The WiFi equipment must be supplied by SPOC and available from the PH2 Catalogue service.
64		Account Management	The WiFi access accounts are managed by SPOC, they are different to the user's domain accounts. The RFCA must request the accounts and then the user maintains them, supported by SPOC.
65		Service Management	The initial cost of setting up the WiFi is funded by the RFCA (Unless this is changed by CRFCA), the ongoing management of the system is under the main MSP contract
66		System Design & Documentation	Each installation must be supported by design documents that can be approved by SCIDA and accreditation authority.
67	Security Management		The MSP is responsible for delivering the physical and configuration security layer of the whole system. This is validated by various checks which are managed by CRFCA.

68		Security Working Group	The terms and references for the Security Working Group (SWG) are managed by CRFCA, guided by the SAC. SWG is chaired by CRFCA (Assistant Director CIS) and membership is agreed as per the terms and references. SAC is a permanent member of the group.
69		Volunterability Assessment	The VAs are carried out by external body and hosted by the MSP. Any observations that require follow up action are managed by CRFCA.
70		Penetration Test	The Pen Tests are carried out by external body and hosted by the MSP. Any observations that require follow up action are managed by CRFCA.
71		SyOPs	CRFCA are responsible for drafting the SyOPs which are reviewed by the SAC. CRFCA can request assistance from the SAC or the MSP if the need arrises.
72		Risk Management & Accreditation Document Set	The RMADS are drafted by the SAC
73		Cyber Protection	The MSP is responsible for ensuring that the agreed cyber protection measures are implemented and maintained. These will be agreed between the SAC, System Architect, Accreditor, JCU and CRFCA.
74		Privilege Access Management	MSP is responsible for the management and control of ALL Privilege Access accounts, including domain admins, local admins, service accounts and the RSAs. The RSAs' use of the privilege accounts must be agreed with CRFCA.
75		Information Security	The MSP, Architect and the SAC are responsible for delivering information security and advising CRFCA of the impact on the system and users. Information Security assurance is delivered through measures and mitigations agreed in the RMADS
76	Asset Management		The Customer is assisted by the MSP in asset management by providing a cradle to grave solution. The MSP provides the system assets (user devices, servers etc, but not printers) and the MSP is responsible for the safe disposal after they have been decommissioned.
77		WEEE Disposal	Dispose of the hardware in line with the latest MOD policy on WEEE disposal.
78		Asset Registration	On setting up a new device for the user or the system, SPOC is responsible for registering the asset in the UAC and the AD.
79		Asset Allocation	The new asset is allocated to the user as specified by the RSA through UAC
80		Warranty Management	MSP supplied equipment's warranty is managed by SPOC. If any equipment needs to be returned to the vendor, the MSP is responsible for secure data deletion and replacing the equipment while it is being repaired. SPOC is NOT reponsible for warranty of any item not supplied by the MSP
81		Secure Data Device Disposal	Assets to be disposed are collected by SPOC from each RFCA's location **twice a year.** Additional Arrangements can be made, at cost. These items are brough to SPOC, storage and RAM is removed and securely disposed of in line with the latest MOD instructions (JSP) and the metal is disposed of through WEEE approved third party
82	Helpdesk Service		
83		Incident Management	Provide a Level 1 user support helpdesk function that provides the services necessary to resolve the basic issues as quickly as possible. The incidents (requests for support) are received by phone, email, online, chat and face to face. However, most users prefer to call and expect to recieve immediate support. More details in the document.

84		Remote Support	The SPOC staff (L1-L3) are able to connect to the user's machine and help to resolve the reported issue. This is done from within the customer's network and the connection and not routed overe
85		Problem Management	SPOC staff escalate incidents to Problems as per the ITIL methodology and then manage those problems to resolution. All related incidents are added to the problem and once the problem is resolved, all incidents are also resolved and the senders notified.
86		Automated Events Management	The PSA and RMM software used by the MSP identifies the events generated by the monitoring systems and create incidents (tickets) automatically for SPOC to address. Tickets can also be resolved automatically if the corrective measures have been applied.
87		Stats Reports	MSP is reponsible for generating the SPOC stats for ISMB and MISB that illustrate the number of incidents, type and success. Any major issues should have specific reports to explain the event in clear language for non technical recepients to understand.
88		Requests Management	Users are able to make requests for resources, training or information through the PSA software. These are treated same as incidents (service tickets).
89		Access Management	Users are able to request access to data or resources, depending on acceess request type and the data, SPOC will either grant the access or escalate the requesd to a business authority.
90	SLA Management		The SLA is agreed to meet the business and financial needs. It covers the service performance and the required support for the policies and procedures. The tollerance levels of non compliances and related penalities are mutually agreed.
91		KPI Reports	MSP is able to provide a pre-agreed set of KPI reports as per the customer's requirements. This includes the option to report on the SLA compliance and Tickets analysis.
92		Performance Reports	Performance reports for the KPIs and the SLA activities are available to the customer.
93		General Stats	Stats relating to the support provided and those that can be extracted from the sysem are made available to the Customer.
94		SLA Maintenance	A quaterly review is carried out to ensure the MSP is delivering the service to a satisfactory level. An annual review is carried out and any ammendments to the SLA are mutually agreed to meet the customer's needs.
95	User Management		SPOC provides the service to manage the user accounts from end to end. A user account is created on request through the UAC and it is removed through the same way.
96		User Access Control	The ability of the user to gain access to any data or resource is authorised through the UAC and actioned by SPOC. This is also checked against the system policies by SPOC.
97		Training	Each user must be provided induction training and various ongoing training as per the customer's traning needs. The MSP is able to provide all system related training and any custom training is defined by the customer and can be delivered by the MSP on mutually agreed terms.

98		Compliance	The user must adhere to the system's needs for security and data use. The user must sign and adhere to the Security Operating Procedures and Responsible For Information training needs. These are checked by SPOC and non-compliance results in access to account being denied.
99		Account Management	Routine checks are carried out to ensure all current accoutns are valid. Any account not used for 3 months is automatically disabled and any account not used for 90 days is automatically deleted, unless it is protected for business or technical needs.
100	Log Management		The key logs generated by the system are used to maintain security, system performance, availability and access.
101		User Devices	All user devices are monitored through logs collected and analysed using the approved software such as Managengine Event Analyser and AD Audit. These logs are reviewed by SPOC daily and any immediate action is managed through incident management, any patterns requiring further management are passed to the ISMB for further direction. The MSP selects the Event to monitor that deliver the customer's requirements for system security, performance and availability.
102		Network Devices	All network devices are monitored through logs collected and analysed using the approved software. These logs are reviewed by SPOC daily and any immediate action is managed through incident management, any patterns requiring further management are passed to the ISMB for further direction. The MSP selects the Event to monitor that deliver the customer's requirements for system security, performance and availability.
103		Servers	All servers are monitored through logs collected and analysed using the approved software. These logs are reviewed by SPOC daily and any immediate action is managed through incident management, any patterns requiring further management are passed to the ISMB for further direction. The MSP selects the Event to monitor that deliver the customer's requirements for system security, performance and availability.
104		Data Centre	The key functions in the data centre, including air con, UPS, Power, Fire, Security are monitored through logs collected and analysed using the approved software. These logs are reviewed by SPOC daily and any immediate action is managed through incident management, any patterns requiring further management are passed to the ISMB for further direction. The MSP selects the Event to monitor that deliver the customer's requirements for system security, performance and availability.
105		Security Systems	Logs from all security systems, firewalls, load balancers, security servers are monitored and approprite and immediate action is taken by SPOC to protect the system from any external and internal threats.
106		Internet Connectivity	Access to the internet is enabled through proxy servers and logs are monitored on the proxy servers and the firewalls. These can be used to track unauthorised uses of the system as well as to protect the system from cyber threats.
107	Network Management		PH2 is a complex network with a large number of local area networks that are joined by VPNS to form the Intranet. These need to be managed to deliver a secure and capable system that meets the user needs.

108		Firewalls	Watchguard firewalls are used to secure the network traffic. The policies are controlled by the MSP to deliver the level of protection agreed in the RMADS. A central management system is used to configure all firewalls.
109		Switches	Cisco and Brocade swithes are used to provide the network connectivity. These are centrally managed and configuration is under configuration management control
110		Load Balancers	KEMP load balancers are use to provide the required load balancing for selected applications and also to provide pre-authentication and reverse proxy function at the system boundry.
111		Management Appliances	Watchguard fiewall manager along with watchguard Dimension are used to monitor the network security and performance.
112		Policies	The MSP is responsible for designing the firewall policies to meet the security requirements agreed in the RMADS and to ensure best security and performance of the system. The external facing firewalls are under strict configuration control. Any major change in policy is tested and agreed with the customer and the accreditation authority.
113		Broadband Management	SPOC is reponsible for maintaining and for ongoing management of the broadband service to the customer sites. Broadband service is used at minor sites only, this includes most ACF sites. Their availability and performance is constantly monitored by SPOC.
114		BT Net (WAN) Management	All RFCAs and some ACFs have BT Net leased line option for their WAN connection into the Intranet. These services are managed by the MSP and maintained by SPOC on day to day bases. Their availability and performance is constantly monitored by SPOC.
115	Data Centre Management		The data centre management is carried out by the MSP, including all responsibilities in relation to it's availability, security and performance.
116		Maintenance Management	Technical maintenance is carried out by a third party, the MSP is responsible for liaison with the third party for routine and any emmergency maintenance. The cost of annual maintenance contract is funded by the customer through SE RFCA.
117		Security Management	The data centre security is managed by SPOC. Access to the data centre, CCTV and fire alarm are also managed by SPOC.
118		Services Management	All services to the data centre are managed by the MSP through liaison with SE RFCA. Including power, maintenance, cleaning, generator fuel, communications, alarms and access control
119		Design Support	MSP is reponsbiel for the design, configuration and upgrades to the data centre
120	BCP Support		The CRFCA Business Continuity Plan includes provision for the CIS DR solution. The data centre is located at SERFCA in Aldershot and the DR site is located at CRFCA in London. The MSP is responsible for maintaining the DR currency as per the business requirements specified by the CRFCA.
121		DR Site Infra Management	The DR site infrastructure is managed by CRFCA and supported by the MSP where needed. This includes assistance in design, specifications and site visits to maintain the DR equipment.

122		DR Management	The MSP through SPOC is responsible for ensuring that the main site is backed up to DR site to meet any challenges documented in the CRFCA BCP/DR Plan. These include the possiblity of total loss of the data centre services.
123		DR Design	The DR design to support the business needs and the agreed DR functionality is the reponsiblity of both CRFCA and the MSP.
124	MDM		Mobile Iron is used as the MDM system to provide the necessary protection for the mobile used by the customer. Only IOS devices are approved for use however some Android devices might could exist without a full MDM rule set being applied. This use of Android and associated risk (not fully managed) is accepted if authorised by CRFCA.
125		System Design	MDM solution is designed by the MSP and installed on premeses to comply with the customer's security policies
126		Manage Devices	SPOC is responsible for managing all mobile devices through the MDM system. The use policy is approved by CRFCA
127		Manage Configuration	MDM configuration is managed through Apple Manager running on Apple Mac. The configuration cannot be changed by the user. Any changes to the configuration are managed through RFC/CAB
128		Manage Installation	These devices are placed in 'supervised' mode by SPOC, the ISO device must be connected to the ISO Manager Mac at the time of MDM installation. This is normally done at SPOC however CRFCA can authorised site visits if a large number of IOS devices are to be brought into service at a time.
129		Manage Policies	All policies are agreed with CRFCA and managed by SPOC. The IOS devices are protected at the same level or higher than user laptops
130		Apps Catalogue	The protected devices are configured to obtain authorised Apps from the PH2 Apps Catalogue. These Apps are approved by CRFCA as required by the business
131	Configuration Management		PH2 system requires configuration management for all systems in use. This includes physical devices, software and policies
132		CMDB	SPOC maintain a Configuration Management Database in the SPOC SharePoint. All approved configuration documents are checked in/out and access to the CMDB is limited to contributors and other authorised users.
133		Policies	The policies for CMDB are defined by the MSP in support of the need to meet the customer's DR and security, and good management requirements.
134		Reviews	All RFCA/Changes result in reviews of the associated CMDB items and any change is subjected to impact analysis. Major security risks, including firewalls are reviewed each year to ensure the physical policies are as per the CMDB records.
135	Internal Audits Support		The systems are subjected to various internal audits and the MSP provides the necessary support where required.
136		CRFCA	CRFCA audits are required to comply with any standard (ISO) that migth be in use, or as result of an incident, or because some validation is required. These audits could be on number of users, user accounts, software in use, devices in use, policies in use, system performance or prior to another type of audit.

137		DIA	CRFCA requests regularly requests the DIA to carry out CIS audits. The MSP provides support and evidence to the audit to confirm the policies and actual working practices used by SPOC and the system users. Any observations and follow up action are managed by CRFCA, corrective action on the CIS, is carried out by the MSP.
138		GDPR	CRFCA is responsible for ensuring that the CIS is in compliant with the GDPR. This can result in audits to be carried out and supported by the MSP
139		RFCA	Each RFCA can request audit of their systems and users. SPOC is required to provide reasonable support as authorised by CRFCA
140		SPOC	The MSP carries out its audits through SPOC to ensure the contractual requirements are being met or need to be changed.
141	Freedom Of Information Requests Support		PH2 system is subject to FOI requests, which are received by CRFCA directly or through the MOD. These could require SPOC to conduct various investigations and reports. There are no special tools in place. The MSP is expected to use the availability capability of standard applications and technical skills to conduct the required action. All systems are subject to this task, including SharePoint, FileStore, Exchange and custom applications managed by the MSP. The customer does not require backups to be searched for the FOI data, this is limited to the online systems only.
142	GDPR Compliance		PH2 system is subject to GDPR requests, which are received by CRFCA directly or through the MOD. These could require SPOC to conduct various investigations and reports. For GDPR purpose.. The MSP is a data processor.
143		GDPR Compliance Systems Support	The PH2 system is required to be compliant with the GDPR policies for data protection and good system management practices. The MSP is responsible for ensuring these requirements are met, or inform CRFCA where they cannot be met and why.
144		GDPR Requests Support	There are no special tools in place. The MSP is expected to use the availability capability of standard applications and technical skills to conduct the required action. All systems are subject to this task, including SharePoint, FileStore, Exchange and custom applications managed by the MSP. The customer does not require backups to be searched for the FOI data, this is limited to the online systems only.
145	**System Management (See SM Map)**		**Items below belong to the central function of system management.**
146			
147	System Management		The MSP is responsible for managing the whole system under an agreed SLA
148	Third Party User Applications Support		The applications are in addition to the standard build suppied by the MSP or in addition to the standard hosted applications provided under contract by the MSP.
149		Sage Payroll	Sage Payroll is installed as a network application in PH2 on a virtual windows server. The client software is available to the user through a thin app type configuration. The user's virtual machine does not have the client installed. The licence is owned by the RFCAs, it is possible that this might change and the licence could be held by CRFCA in the future.
150		Sage HR	Sage HR is installed on a virtual server in PH2E and can be accessed by all users if required.

151	Mapthat	NO LONGER IN USE
152	ISOMA	ISOMA is a process building graphical applications used by the RFCAs to map out various processes. The MSP's task is to maintain the server and assist with updates. The Vendor does not have direct access to the system, they must go through SPOC.
153	MOD Applications - Connectivity Support	The MOD applications hosted on the RLI have various configuration requirements, either in the browser or on the client and also the version and type of client OS, services and configuration. SPOC is required to assess the technical needs and configure the virtual networks so that they are able to run the applications successfully.
154	Symphony	Support for symphony requires the MSP to be responsible for every aspect of hosting an application, including ensuring that it meets the needs of high availabiilty. The Vendor is responsible for the application development and updates to the application. It is a an ASP application that uses an ORACLE backend database. The system backups and the high avaiability configuration of SQL Always On are all necessary.
155	DRM - SalesForce	SalesForce is a web CRM application that DRM use. SPOC is reponsible for it's availability through networking only. SPOC or the MSP are not responsible for what goes on inside SaleForce. Access to the SalesForce application data for DRM is limited by IP Addresses in Pardot managed by DRM
156	DRM - Pardot	Pardot is a web markeing application that is within the SalesForce framework and it is for DRM use. SPOC is reponsible for it's availability through networking only. SPOC or the MSP are not responsible for what goes on inside Pardot. Access to the Pardot application data for DRM is limited by IP Addresses in Pardot managed by DRM
157	Colligo	Colligo application allows the PH2 virtual desktop user to save emails into SharePoint. It is integrated with the Office installation on the Virtual Desktops in PH2. MSP provides the service to integrated, maintain, training.
158	Acrobat Reader Professional	This application is used by a few users in PH2E and it is installed on their physical desktops/laptops. MSP is responsible for installation, maintenance, upgrades and training where required.
159	MS Project	This application is used by a few users in PH2E and it is installed on their physical desktops/laptops. MSP is responsible for installation, maintenance, upgrades and training where required.
160	Autocad	This application is used by a few users in PH2E and it is installed on their physical desktops/laptops. MSP is responsible for installation, maintenance, upgrades and training where required.
161	Autocad Light	This application is used by a few users in PH2E and it is installed on their physical desktops/laptops. MSP is responsible for installation, maintenance, upgrades and training where required.
162	Photoshop	This application is used by a few users in PH2E and it is installed on their physical desktops/laptops. MSP is responsible for installation, maintenance, upgrades and training where required.
163	Local Access Database Applications	RFCAs use Access Databases to maintain lists of local contact and community engagement campains. These are used in PH2E and PH2. MSP provides support as requested.

164	Client Applications Support		These applications are installed on the users' client machines in PH2 and PH2 virtual desktops, MSP provides support for installation, configuration, maintenance, upgrades,training and general use advise as requested
165		Word	Most users only make basic use of the application. A few users require advance support, including debuging of issues and use of advance features in addition to the basic training provided through SPOC
166		Excel	Most users only make basic use of the application. A few users require advance support, including debuging of issues and use of advance features in addition to the basic training provided through SPOC
167		PowerPoint	Most users only make basic use of the application. A few users require advance support, including debuging of issues and use of advance features in addition to the basic training provided through SPOC
168		Access	Most users only make basic use of the application. A few users require advance support, including debuging of issues and use of advance features in addition to the basic training provided through SPOC
169		Outlook	This is the most used application. A few users require advance support, including debuging of issues and use of advance features in addition to the basic training provided through SPOC
170		Inter Explorer	Use of IE is managed through GPOs which enforce a strong set of security controls. Users need help to debug issues when they are not able to access specific applications. All traffic is routed through proxy servers
171		Google Chrome	The use of Chrome is forced through the need to use some applications that are not supported in IE. MSP takes care to protect the system for unauthorised use of chrome features through best practice configuration and SyOPs.
172		Publisher	This aplication is used by a few users and requires little help.
173		Acrobat Reader	This is the standard application for opening PDF documents. It is kept up to date along with MS software updates.
174	Level 1 User Support		First point of contact for all Incident related to the use of system. Troubleshoot, research, diagnose, document and resolve issues where possible, within windows OS and installed applications. Where an issue cannot be resolved, it is excalated to Level 2 or 3 or dealt with by another way within the ITIL framework of system support. Build (software) user machines on demand, rebuild machines when required. Process orders and requests for new equipment and training. Record all activities against SLA.
175	Level 2 System Support		Monitor System status using the tools available to the MSP and address issues escalated by Level 1, including configuration, printing, access controls, system errors. Also monitor network and escalate issues to the Level 3 network team if required. . Process orders and requests for new equipment and training. Record all activities against SLA.
176	Level 3 System Support		Address issues escalated by Level 1 and Level 2, involving system level configuration, errors, upgrades, investigations, network troubleshooting, virtualisation environment troubleshooting. Replace hardware, virtual machines, disaster recovery tasks, R&D, RFCs' impact assessment and completions. Escalate issues to Level 4 or the management as needed.

177		Virtualisation	Maintain all virtual system up to date with software patches, firmware, BIOS upgrade. Design, maintain, upgrade, troubleshoot, VMWare vSphere, vCentre, virtual networking, DR tasks, and every other task necessary to keep the system available for use.
178		Virtual Desktops	Provide virtual desktops using VMWare horizon, as per the design to maintain availability, functionality and security.
179		Hardware	Maintain hardware, through local support and warranty support from the vendors. Monitor performance, upgrade and replace as necessary.
180		Support Software	Maintain the MSP software to manage the system, including logs collection, PSA, RMM, Asset Management and reporting.
181		Backups	carry out backups, daily, weekly, monthly as per the backup (DR) plan. Using, all available backup systems and software. Maintain backup tapes in secure storage off site.
182		Patching	Implement the agreed Patching Policy and upgrade as per the system and security needs.
183		Operating Systems	Maintain Windows OS, Linux, Vmware, up to date and upgrade as necessary.
184		DR Support	Deliver the BCP and DR services as per the agreements. This includes recovering data from routing backups, such as user files, mailbox data or a whole VM. Deliver and manage the DR solution up to and including switchover to a DR site after a major disaster at the live site.
185	Internal DNS		Maintain DNS for all internal service, this is managed on all domain controllers, approximately 75 in PH2E and 4 in PH2.
186	Level 4 Support		Escalate and manage incidents to the vendors.
187	Remote User Support		Remote users connect to the PH2E system over VPN
188		Off Base	Assist in connection to the VPN through hotspots and other difficulties that the user might experience
189		Remote Office	Where a user works alone or with other similar users and without a local firewall to provide a branch office vpn solution. Individual VPNs on devices results in the Users not being able to share data or services between them at the same site
190		ACF Camp	When users are at the ACFs' camps, they are located in areas of poor internet connectivity, which is not managed by the MSP. This results in various challenges that the user requires SPOC support for.
191	Appliances		These appliances are in use within the customer's system
192		KEMP	Load balancer, high availaiblity, reverse proxy, preauthentication.
193		Artica	Proxy server that uses a client ID software on each device to record use of the internet
194		SecureEnvoy	Dual factor authentication for CASTRA and any other similar system that needs to be supported with connections to the internet users.
195		Mobile Iron	MDM software to manage mobile phones in supervised mode
196		Time Manager	Clock! 'Provides support for system time management
197		Avaya Telecom	Avaya server that provides the telecom service to the RFCAs/ACFs - **NOT IN SCOPE OF MPS CONTRACT**
198	Server Management		SPOC is able to manage these server types
199		WSUS	Maintain the Windows Updates configuration to ensure all supported windows OS and applications are supported through this system

200		KMS	License manager for MS products. Maintain the licences and troubleshoot issues.
201		Exchange	Managa MS Exchange in high availability DAG and multi edge servers environment. Manage Performance, updates and security, including SPAM and other Cyber threats
202		SharePoint	Manage multiple SharePoint farms, with front end servers, application servers and SQL always on. There are large number of SharePoint sites and site collections that must be maintain daily. Provide support for custom configuration, including sharepoint development for custom applications.
203		SQL	Manage SQL DBs, installation, maintenance, manage always on high availability and DR tasks.
204		FileStore	Manage multiple uses of windows server as filestore. Use DFSR to sych the data between 75+ servers for DR and availability. Manage Dedup, security, access control and storage availability.
205		Application Server	Applications Servers are used for custom applications, SharePoint, ORACLE Applications.
206		Windows 2012	Maintain Windows Server 2012 OS
207		Windows 2016	Maintain Windows Server 2016
208		VMWare Connection	VMWare Connection Servers are used for Horizon VDI
209		VMWare Security	VMWare Security Servers are used in the PH2 DMZ for pre-authentication and processing connections to virtual desktops
210		VMWare vCentre	Multiple instances of vCentre to manage the virtual environement.
211		VMWare Composer	Composer is used by VMWare VDI to deliver desktops
212		DHCP	DHCP servers are used to manage IP address allocations with VDI . In PH2E, DHCP function is managed by the local firewalls
213		Skype For Business	Skype For Business use is growning and provides enterprise solution for IM, Screen and document Shareing, Video Conf and Audio connections as on prem installation
214		Web Applications	MSP provides support fo the business web applications developed in Dot net, PHP, C#, HTML
215		RFCA Cloud	RFCA Cloud is data sharing solution that uses Own Cloud technology
216	Internet DNS		Manage the domain DNS published on the internet for all domains in use. The .mod.uk domain DNS are managed by the MOD webmaster and liaised by the MSP
217	System Applications		These applications run on the system in support of the MSP tasks
218		PostCode Plus	Used by Alternative Venues, PQQ and other custom applications. MSP maintains the database and patching as provided by the supplier
219		SMS	Bulk SMS system is used to send SMS messages during system failure when other systems are not available. MSP maintains the user contact details.
220		ControlPoint	ControlPoint is used to manage and provide reporting on SharePoint permissions and usage on both farms, PH2 and PH2E
221		Event Logs	Event Logs software monitors all events on the managed devices, including user device and all servers. The output is monitored by the MSP and appropriate action taken as required.
222		AD Audit	Active Directory Audit software is used to mange the AD configuration and use

223		McAfee AV	McAfee AV is installed on all PH2E devices
224		McAfee DLP	Data Loss Prevention software is use to lock USB ports on user devices. It is managed through controlling the Users' access level and not based on device. An authorised user can use USB devices on any connected machine.
225		VEEAM	VEEAM is used for routine backups and DR tasks as well as for DR synchronisation between the main and DR sites
226		Carbonite	Carbonite is used to Sych VMs between the main and DR site
227		BackupExec	BackupExec is used for daily backups and DR tasks to recover the data
228		TrenMicro AV	TrendMicro is used in PH2 for servers and Virtual Desktops.
229		Blancco	Blancco is the MOD standard software for secure deleting of data on drives before disposal or re-use
230	Active Directory Management		AD provides the necessary security layer for the system and is managed through policies and configuration
231		Distribution Groups	These are used to create groups for communications, emails and other messages
232		Group Policy Objects	A large number of GPOs are needed to implement the required security policies
233		Security Groups	Security Groups are used to define a group of users that require same access levels. PH2 makes heavy use of security groups for SharePoint and Filestore access permissions.
234		AD Accounts	User accounts and contacts are created and managed in line with the PH2 access policies. Username formats are agreed at MISB and executive level.
235		AD Security	AD security is enforced using security certificates that are self signed and commercially purchased. Access to AD management is limited to SPOC and RSAs who are required to adhere to the Admin SyOPs
236		User Groups	User groups are created to manage access and communications
237		AD Forest	PH2 and PH2E are managed within their own independent AD forests.
238		Devices	All authorised devices that connect to the domain are added to the domain by SPOC only
239		Distributed File System Replication	DFSR is used to synch data between local and central servers for backup, access and DR
240		Domain Controllers	Each site has its own domain controller that is part of the AD forest in PH2E. PH2 has domain controllers in the main and DR site
241		Organisational Units	Each RFCA and ACF unit is allocated to its own OU
242		LDAP	LDAP is used to integrated with other systems for dual authentication and custom applications
243		Security Account Management (SAM)	AD is configured to allow use of SAM and system policies are used to prevent unauthorised use or cyber attacks through use of AV and event logs
244		LDAPS	LDAPS is configured in PH2 and used between VMWare and Windows domain
245		Domains	MSP is responsible for day to day of domain management. There are two AD domains (PH2 and PH2E), and various internet domains for public facing applications that are managed by the MSP