Appendix 1: SSRO-C-134 Specification - SSRO IT managed service (ITMS) and DefCARS contract

November 2024

Contents

SSRO-C-134 Specification - SSRO IT managed service (ITMS) and DefCARS contract

Background to the ITMS and DefCARS contracts

1. The Single Source Regulations Office (SSRO) is an executive non-departmental public body, sponsored by the Ministry of Defence (MOD). The SSRO currently has 40 staff members, alongside 10 non-staff members (Board / panel members). In addition, there are test and administration, third-party user accounts and devices and third-party and MOD guest user accounts. Guest access is also provided for currently around 500 MOD users (for access to Power BI and some SharePoint sites), and a small number of other trusted parties (e.g. Finance system supplier, Government Internal Audit Agency).

2. Our office is based in the Government Office Great George Street, 100 Parliament Street, London. Further information about the SSRO can be found on its website: Single Source Regulations Office - GOV.UK (www.gov.uk). Staff regularly work from home (and around a quarter of staff are designated as full-time home workers) as well as occasionally from other locations (for example while travelling; from hotels; from defence contractor and MOD sites; and very occasionally while abroad). Staff use laptops (Dell and MS Surface), and iPhones, and non-staff users use iPads or laptops.

3. The SSRO has a contract for the provision of its Defence Contract Analysis and Reporting System (DefCARS). DefCARS is a secure, online system for the capture, storage and analysis of all electronic data reported by defence contractors under the Defence Reform Act 2014. DefCARS is accessed by industry, the Ministry of Defence (MOD) and the SSRO. Further information on DefCARS is on our website.

4. We currently have two contracts in scope for this RFI to meet the SSRO's IT requirements:

    a. a core ITMS (including a virtual Security Operations Centre (SOC)) contract. This is due to end on 24 March 2026, but has an option to extend by a further year; and
    b. a support and development of DefCARS contract. This is due to end on 9 January 2026, but we are considering options for a coterminous date with the ITMS completion date of 24 March 2026.

5. We have a New Commerce Experience (NCE) contract for the provision of Microsoft licenses and Microsoft cloud services. The provision of these licenses is not in scope for this RFI.

6. The SSRO's ITMS is cloud based and uses the Microsoft stack. Third parties are used for management, support, and development of the IT environment. The SSRO technology and systems estate includes the SSRO Microsoft environment which is based in UK data centres. Connectivity within our office is via Wi-Fi only, provided by the Government Property Agency through the GovWifi service. The GPA also provide a network printing service, GovPrint, connecting to a Xerox printer over GovWifi.

7. During August 2021 the SSRO implemented a zero-trust connectivity architecture using the iboss cloud platform (iboss.com). Infrastructure, Iboss and Microsoft logs including Defender for Endpoint and Defender for Cloud logs are monitored by a 365/24/7 SOC.

Cloud based print management is provided by Gov Print. Intelligent phishing protection is provided through the latest Microsoft tooling. Backup of the Microsoft 365 environment, in addition to Microsoft backup services, is provided by Datto Backupify. This includes SharePoint, Exchange and OneDrive for Business. Non-Microsoft applications installed on devices include Adobe Acrobat (Reader and Pro), Adobe Illustrator and Adobe InDesign. The SSRO also use a single Bloomberg terminal installed on a Windows desktop PC.

8. The SSRO Microsoft environment is included in the scope of the security accreditation of DefCARS by the Ministry of Defence's Cyber Defence and Risk team (CyDR). The ITMS supplier will be responsible for activities in support of security accreditation including supporting an independent IT Health Check and taking any remedial action required. This covers the cloud platform underpinning DefCARS, M365 and Azure.

9. Our Azure tenant holds two subscriptions, one for core IT services and one for the DefCARS web application. The core IT service subscription includes DefCARS elements in Power BI and Azure DevOps. Management of the overall Azure tenant and core IT subscription (including M365 and the DefCARS elements in Power BI and Azure DevOps) is the responsibility of the ITMS supplier. The DefCARS subscription is managed and supported by the DefCARS supplier.

10. Our current Azure costs are approximately £60,000 per annum excluding VAT. The majority of Azure services are for DefCARS, including Log Analytics; Azure App Services; Application Gateway; Power BI Embedded; SQL Database; Synapse Analytics; Purview; and Data Factory.

11. We have reviewed the scope across the two contracts and the current service requirements and are considering a procurement exercise during 2025, for a three-year contract (with the possibility of two +1 extensions beyond that) using the possible following approaches:

    a) combine the ITMS (including SOC) and the DefCARS scopes of work under a single contract; or
    b) combine the ITMS (excluding SOC) and the DefCARS scopes of work under a single contract and procure a separate and independent SOC; or
    c) continue to procure the ITMS (including SOC) and the DefCARS scopes of work under two separate contracts; or
    d) procure the ITMS (excluding SOC) and the DefCARS scopes of work under two separate contracts and procure a separate and independent SOC; or
    e) procure the ITMS (excluding SOC) and the DefCARS scopes of work (excluding development tasks) in one contract and procure a separate and independent SOC and a separate contract for DefCARS development tasks.

12. Annex A provides further information on the current SSRO ITMS estate and Annex B provide further detail on DefCARS. We are seeking input from potential bidders on any or all of the above approaches. Annex C and Annex D to this document set out more details of the specification requirements for the ITMS and for DefCARS respectively. These requirements are broadly drawn from the existing specifications for our contacts and will be updated in due course for any actual future procurement that the SSRO runs. The requirements are provided to give context about the two existing contracts.

Annex A- Current SSRO ITMS estate overview

This annex broadly outlines the current ITMS estate and will need to be updated in due course for any actual future procurement that the SSRO runs. This information is provided to give context about the current contract.

End User Devices and Peripherals

Device	Make and Model	Quantity
Laptops	Dell XPS 13 with docking station	30
	Dell XPS 15 with docking station	10
	Microsoft Surface Pro with docking station	2
	Microsoft Surface Book with docking station	4
Desktop PC	Dell Precision 3660	1
Mobile devices	iPhone 14	1
	iPhone 13	2
	iPhone 12	14
	iPad Pro 10.5" 64gb – Wifi only	3
	iPad Pro 11" 3rd gen 128gb – Wifi only	3
Mac Mini Desktop	For configuring the above	1
Monitors	Dell 24” LED	42
Wireless Headsets	Jabra Evolve 65 & Stealth	One per each member of staff
Webcams	Logitech C930e	20

Infrastructure Equipment

Device	Make and Model	Quantity
Printer – Office, USB connection	HP Laserjet P3015	1
Printer – Home Worker	Brother MFC-J4420DW	1
	HP OfficeJet Pro 8720	1
	HP OfficeJet Pro 9010	1
	Canon PIXMA MG2551S	1

Office 365 Data

- SharePoint: 250,000 files stored, 1.2TB of 1.6TB of data used
- OneDrive: 200,000 files stored, 130GB of data used
- Exchange: 54 active mailboxes, 115GB of storage used
- Teams: 33 Teams

Core common desktop services:

- Windows 11, Office 365 including SharePoint Online and Power BI
- Microsoft Visio, Microsoft AIP Office Add-ins
- Microsoft 365 E5 licenses, plus domestic Teams call plans
- Google Chrome, Microsoft Edge
- Adobe Acrobat Reader
- iBoss Client
- Ciros Client (gov print)
- Bitlocker device encryption, Windows Defender AV
- Intune client

Business Applications:

- Adobe: InDesign CC, Adobe Acrobat Pro & Illustrator CC
- Microsoft Project
- Zoom: Free version installed for joining external meetings
- DefCARS (including PowerBI and Azure DevOps in core IT subscription)
- SQL tools: Microsoft SQL Server Management Studio, Microsoft SQL report builder and Microsoft Visual Studio SQL Server Data Tools
- Bloomberg terminal: Office based Desktop PC accessing Bloomberg financial services application
- ShareGate: One licence, installed on an Azure VM
- R, including R add-in for Power BI, used for statistical analysis

Web based business applications:

- Convene: Web based application which provides access to electronic board papers. This is also an app on corporate iPhones and iPads.
- People HR: Human Resources web-based application

- Smart Survey
- Finance Tools: Expensify, used for processing expenses; Iplicit, accounting software also used for processing PO's and invoices. For both of these there is also an app on corporate iPhones and iPads.

Current Microsoft Licences (via NCE)

Product Title	Total Licenses
Communications Credits	Unlimited
Microsoft 365 Audio Conferencing	1
Microsoft 365 Domestic Calling Plan	12
Microsoft 365 Domestic Calling Plan (120 min)	35
Microsoft 365 E5	50
Microsoft 365 Phone System - Virtual User	4
Microsoft Power Automate Free	10,000
Office 365 E1	4
Office 365 E3	2
Office 365 E5	1
Power BI Pro	2
Project Plan 3	1
Rights Management Adhoc	50,000
Visio Plan 2	2

Licences supplied through our current ITMS supplier that will need to be provided by the Supplier:

- Datto Backupify (or alternative)

Current Azure Services

Core IT: All are located in the UK South data centre within the same Azure subscription.

Service type	Description	SKU(s)
Virtual Machine	Windows (Windows Server 2022 Datacenter), UK South Disks: 64 GiB Standard SSD LRS (500 MaxiOPS 60Throughput 16Gib Standard SSD LRS (500 MaxiOPS 60Throughput	Standard B2ms (2 vcpus, 8 GiB memory)

	1 private IP address	
VPN Connection	Gateway Type: Basic, policy-based VPN type. 1 Public IP address	Basic
Storage Account	Storage (general purpose v1) Primary/Secondary Location: Primary: UK South, Secondary: UK West Geo-redundant storage (GRS), standard performance	Storage (general purpose v1)
3x Storage Account	StorageV2 (general purpose v2) UK South Locally redundant storage (LRS) Performance: Standard	StorageV2 (general purpose v2)
Storage Account	Storage (general purpose v1) UK South Locally redundant storage (LRS) Performance: Standard	Storage (general purpose v1)
Public IP address (x3 of these)	Tier: Regional Location: UK South (Zone 1, 2, 3)	Standard
Recovery Services Vault	n/a	n/a
Bastion	UK South	Basic
Azure DevOps	n/a	n/a

DefCARS Azure services (in separate Azure subscription to Core IT services. All will be located in the UK South data centre):

ServiceFamily	ServiceName	Meter
Databases	SQL Database	vCore
Analytics	Azure Synapse Analytics	100 DWUs
Analytics	Power BI Embedded	A1 Node
Networking	Application Gateway	Fixed Cost
Management and Governance	Log Analytics	Pay-as-you-go Data Ingestion
Analytics	Azure Purview	Standard Capacity Unit
Compute	Azure App Service	P1 v3 App

Analytics	Azure Data Factory v2	Cloud Data Movement
Analytics	Azure Purview	Data Map Enrichment - Data Insights Generation vCore
Compute	Azure App Service	Standard SSL - 1 Year Certificate
Compute	Azure App Service	B2 App
Networking	Application Gateway	Capacity Units
Databases	SQL Database	RA-GRS Data Stored
Containers	Container Instances	vCPU Duration
Security	Advanced Data Security	Standard Node
Analytics	Azure Synapse Analytics	Standard LRS Data Stored
Internet of Things	Event Hubs	Standard Throughput Unit
Security	Security Center	Standard Node
Databases	SQL Database	S2 DTUs
Databases	SQL Database	S0 DTUs
Databases	SQL Database	Data Stored
Networking	Virtual Network	Standard IPv4 Static Public IP
Analytics	Azure Data Factory v2	Cloud Orchestration Activity Run
Management and Governance	Log Analytics	Pay-as-you-go Data Retention
Analytics	Azure Purview	Standard vCore
Management and Governance	Azure Monitor	Alerts Metrics Monitored
Containers	Container Instances	Memory Duration
Containers	Container Registry	Basic Registry Unit
Databases	SQL Database	S1 DTUs
Security	Advanced Threat Protection	Standard Events
Security	Advanced Threat Protection	Standard Transactions
Integration	Logic Apps	Standard Connector Actions
Networking	Bandwidth	Standard Data Transfer Out
Security	Azure Active Directory B2C	Multi-Factor Authentications
Analytics	Azure Synapse Analytics	Standard RA-GRS Data Stored
Databases	SQL Database	Backup RA-GRS Data Stored
Analytics	Azure Synapse Analytics	Azure Hosted IR Data Movement
Databases	SQL Database	B DTUs
Security	Azure Active Directory for External Identities	P2 Monthly Active Users
Networking	Bandwidth	Inter Continent Data Transfer Out - NAM or EU To Any
Storage	Storage	Hot LRS Data Stored
Storage	Storage	Hot RA-GRS Data Stored
Storage	Storage	Read Operations
Analytics	Azure Synapse Analytics	Azure Hosted IR Orchestration Activity Run
Analytics	Azure Synapse Analytics	Azure Hosted IR Pipeline Activity
Analytics	Azure Purview	Data Insights Report Consumption
Analytics	Azure Data Factory v2	Cloud Pipeline Activity
Management and Governance	Azure Monitor	Emails
Integration	Logic Apps	Data Retention

Storage	Storage	Hot RA-GRS Index
Networking	Bandwidth	Intra Continent Data Transfer Out
Storage	Storage	All Other Operations
Storage	Storage	Hot LRS Write Operations
Storage	Storage	GRS Data Stored
Security	Key Vault	Operations
Storage	Storage	Hot GRS Iterative Read Operations
Storage	Storage	Class 2 Operations
Analytics	Azure Data Factory v2	Cloud External Pipeline Activity
Analytics	Azure Data Factory v2	Cloud Read Write Operations
Storage	Storage	Hot GRS Write Operations
Storage	Storage	LRS List and Create Container Operations
Storage	Storage	Hot GRS Data Stored
Storage	Storage	GRS Batch Write Operations
Storage	Storage	GRS List and Create Container Operations
Integration	Service Bus	Standard Messaging Operations
Storage	Storage	LRS Class 1 Operations
Databases	SQL Database	LRS Data Stored
Storage	Storage	Hot Read Operations
Storage	Storage	RA-GRS Data Stored
Storage	Storage	GRS Write Operations
Storage	Storage	LRS Data Stored
Storage	Storage	Batch Write Operations
Internet of Things	Event Hubs	Standard Ingress Events
Storage	Storage	Hot Other Operations
Storage	Storage	Geo-Replication v2 Data Transfer
Analytics	Azure Data Factory v2	Cloud Monitoring Operations
Storage	Storage	Scan Operations
Storage	Storage	List Operations
Analytics	Azure Synapse Analytics	Azure Hosted IR External Pipeline Activity
Storage	Storage	GRS Class 1 Operations
Storage	Storage	LRS Write Operations
Storage	Storage	Write Operations
Compute	Azure App Service	F1 App
Networking	Bandwidth	Standard Data Transfer In
Security	Advanced Data Security	Standard Trial Node
Security	Advanced Threat Protection	Standard Trial Transactions
Storage	Storage	Delete Operations
Storage	Storage	Geo-Replication Data Transfer

Incidents, Requests and Changes

Volumes of Incidents by Priority

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
P2	3	0	1	0	1	0	0	0	1	1	0	0	0
P3	36	31	23	21	24	22	24	30	35	11	25	53	22
Total	39	31	24	21	25	22	24	30	36	12	25	53	22

Top 5 Incidents by Category and Subcategory (recent months)

Category	Count	% of All	Subcategory	Count
MS Azure	9	31.0%	Other	9
MS Outlook	5	17.2%	Profile Issue	1
			Send/Receive Issues	2
			Software Issue	2
Mobile Device	4	13.8%	Device Issue	3
			Other	1
Generic Software	2	6.9%	Other	2
Laptop	1	3.4%	Device Upgrade	1

Volumes of Requests

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
P1	0	0	0	0	0	0	0	0	1	0	0	0	0
P2	0	0	0	0	0	0	1	0	0	0	0	0	1
P3	29	25	19	11	19	19	20	18	39	28	19	28	27
Total	29	25	19	11	19	19	21	18	40	28	19	28	28

Top 5 Requests by Category and Subcategory (recent months)

Category	Count	% of All	Subcategory	Count
Information	13	35.1%	Other	2
			Report	11
User Account Request	8	21.6%	Amend Account Permissions	3
			Amend Group Membership	2
			Leaver Request	1
			New User Request	1
			User Information Update	1
Software	6	16.2%	O365 Licence	1
			Other	1
			Patch Management	1
			Software Install	3
Create SharePoint Document Library	3	8.1%		3
Email	2	5.4%	Mail Release	1
			Mailbox Permissions	1

RFCs by type of change

	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
Emergency	1	0	0	0	0	0	0	0	0	0	0	0	0
Major	1	0	0	0	0	0	0	0	0	0	1	0	0
Minor	1	1	1	1	0	0	2	1	5	0	1	3	6
Retrospective	0	0	0	0	0	0	0	0	1	0	0	0	0
Standard (Pre-Approved)	0	0	0	0	0	0	0	0	0	0	2	0	0

Continuous Improvement history (past months)

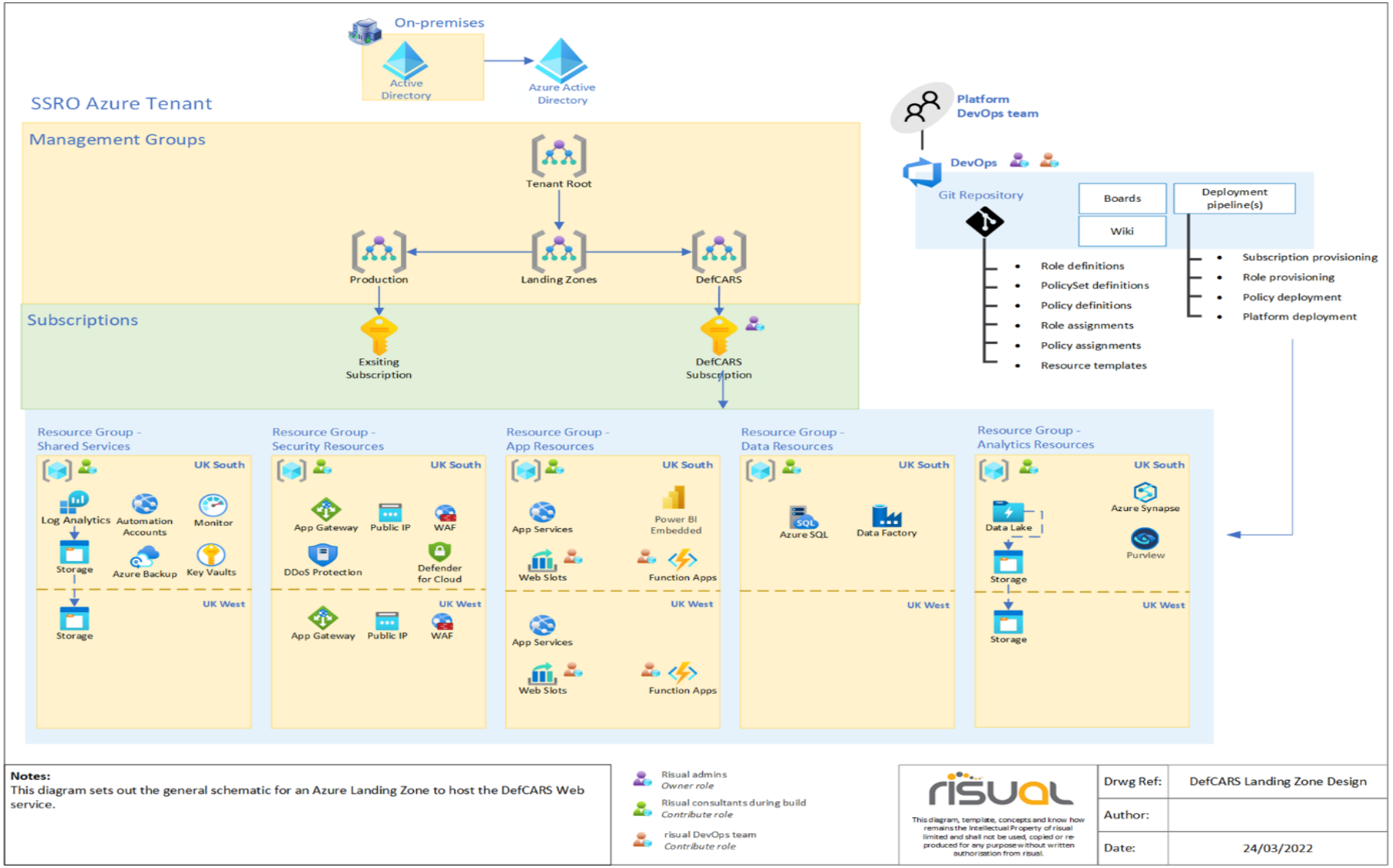
Date Added	Status	Description
Jan 2025	Planned	Information Protection Improvements - Design and Implementation
Jan 2025	Planned	Improvements to SOC service monitoring
Nov 2024	Started	Microsoft CoPilot Assessment Review
Nov 2024	Started	Review and update of InTune management of iOS devices
Oct 2024	Complete	Review of iBoss and potential replacements
July 2024	Complete	Upgrade to Windows 11
June 2024	Complete	DLP policy review
May 2024	Complete	Replace Egress Defend with Microsoft tooling
May 2024	Complete	Phishing simulation configuration
Feb 2024	Complete	Azure optimisation and clean up
Nov 2023	Complete	MFA review and move to authenticator app

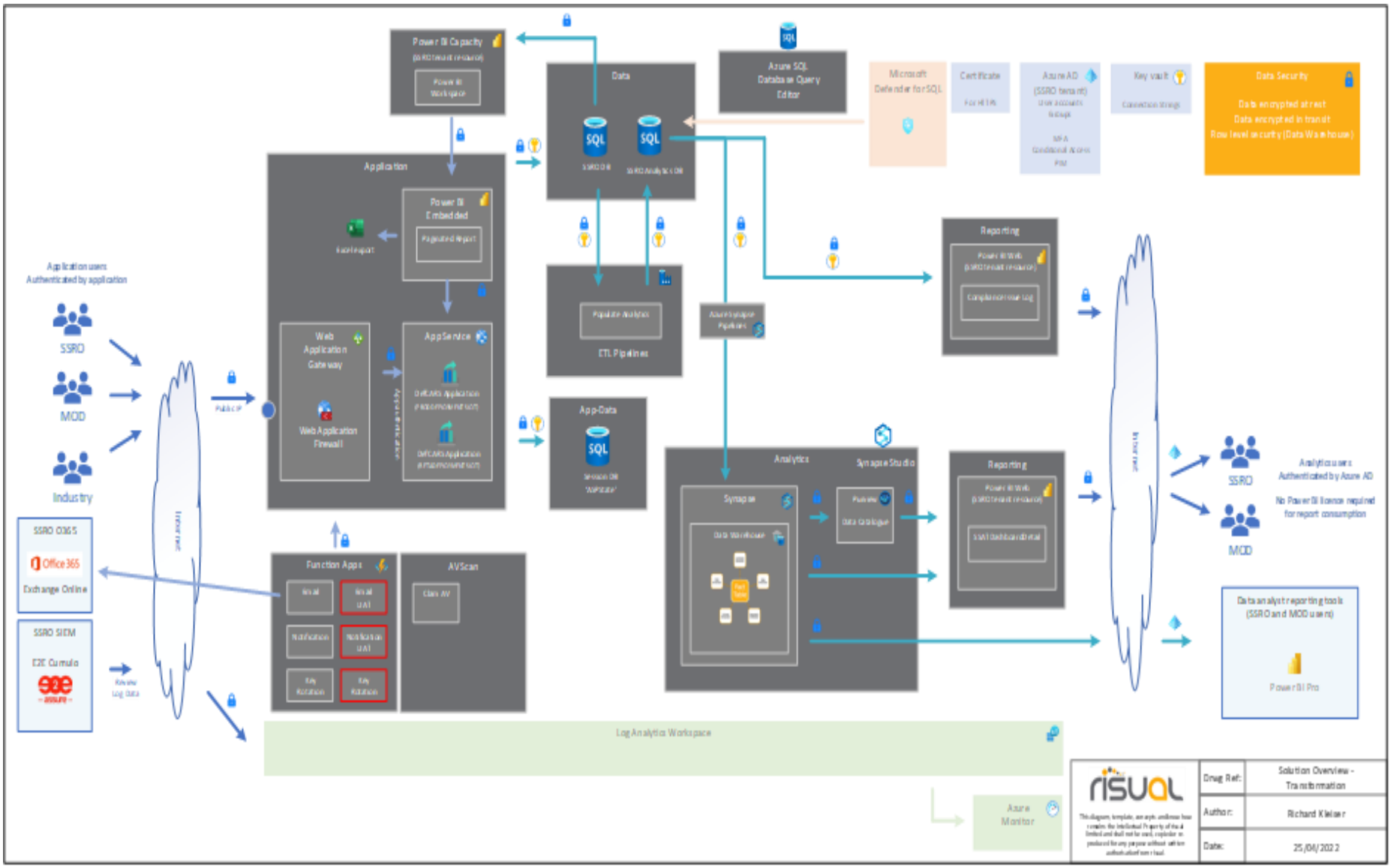
SOC log volumes

	Aug 2024	**Sept 2024**	**Oct 2024**
Raw logs	775,413,443	777,004,651	880,522,105
Events of interest	269,868,948	269,667,387	304,527,569
SIEM alerts	170	205	209
Auto close rule	7	21	29
Ticket (human interaction)	7	3	1
Incident	0	0	2*

*On investigation these were for zero day exploits in products not used by the SSRO

DefCARS Solution Overview




Power BI Capacity
Power BI Workspace
Data
SQL
SQL
Azure SQL Database Query Editor
Microsoft Defender for SQL
Certificate
Azure AD
(SSRO tenant)
Key vault
Data Security
Data encrypted at rest
Data encrypted in transit
Row level security (Data Warehouse)
Application
Power BI Embedded
Paginated Report
Excel export
Web Application Gateway
Web Application Firewall
AppService
Application users
Authenticated by application
SSRO
MOD
Industry
Internet
Public IP
Populate Analytics
ETL Pipelines
Azure Synapse Pipelines
App-Data
Reporting
Power BI Web
(SSRO tenant resource)
Compliance use Log
Analytics
Synapse Studio
Synapse
Data Warehouse
Purview
Data Catalogue
SSAS dashboard/detail
Function Apps
AVScan
Clam AV
SSRO O365
Office 365
Exchange Online
SSRO SIEM
E2E Cumulo
Review Log Data
Log Analytics Workspace
Azure Monitor
Analytics users
Authenticated by Azure AD
No Power BI licence required for report consumption
Data analyst reporting tools
(SSRO and MOD users)
Power BI Pro
risual
Drug Ref:
Solution Overview - Transformation
Author:
Richard Kleiner
Date:
25/04/2022

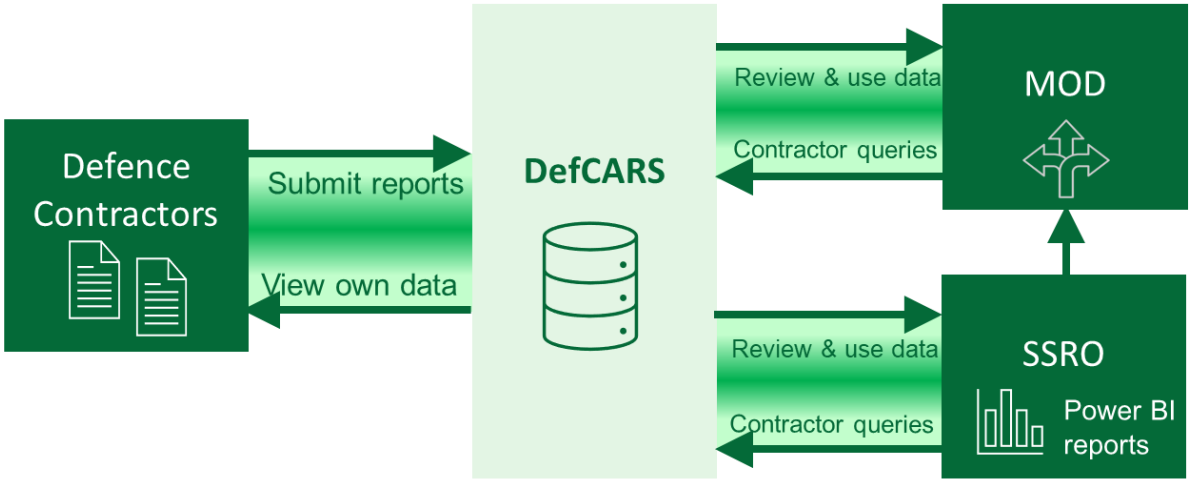
Annex B- Current DefCARS overview

Defence contractors are required to provide reports to the SSRO and the MOD if they hold qualifying contracts under the regulatory framework. The Regulations prescribe the types of reports, their contents and the circumstances in which they must be provided.

The SSRO has established DefCARS as a secure, online system that is easy to use for the capture, storage and analysis of all electronic data reported by defence contractors and suppliers in accordance with the Act and the Regulations. DefCARS is accessed by industry, MOD and the SSRO and it:

- Enables defence contractors to submit statutory reports and access their data.
- Facilitates monitoring of compliance[1] with reporting requirements by the SSRO, and facilitates the review of reports by the MOD.
- Holds reported data and makes it accessible.
- Produces reports and supports analysis of reported data.

Figure 1: DefCARS current functionality



Currently DefCARS consists of a number of databases and services as set out in the diagrams in Annex A DefCARS Solution Overview. Access to the WebApp is delivered via a secure web-based interface to a closed group of users. The system provides for submission of defence contract data at OFFICIAL – SENSITIVE – COMMERCIAL, as defined in the Government Security Classifications May 2018.

The current DefCARS WebApp is a .NET Framework 4.8 WebApp. The WebApp is hosted in Azure and uses the full suite of Azure DevOps services - Boards, Repos, Pipelines, Test Plans and Artifacts to manage the Software Development Lifecycle. The WebApp has a number of supporting Microservices to support its functionality. It is supported Azure SQL databases (production & session state).

[1] Compliance and review methodology 2023 - GOV.UK

WebApp

The WebApp is built in ASP.NET primarily using the following languages:

- C#
- Javascript
- HTML
- cshtml
- CSS

The WebApp primarily composes of a number of Web Forms, along with user access management and metadata management features. The WebApp is comprised of around 350 views, 350 controllers and 550 Class Libraries, there are around 100 packages within the Artifacts feed.

Microservices

The following microservices support the application:

- Azure Application Gateway - Gateway and Web Application Firewall
- Function App (NET 8.0) - Email service for authentication and notifications
- PowerBI Embedded - Provides Excel download reporting capability to users
- Container Instances & Clam AV - Clam AV is a containerised app which provides malware protection for the File Upload feature.

The SSRO published a Technology Strategy in 2021 for DefCARS[2] which set out:

- details of the current system;
- plans to move the system to the public cloud (now complete); and
- future developments to improve the functionality and operation of the system.

DefCARS launched on 15 March 2017 and has received positive feedback from industry, the MOD and the SSRO's users. The current database replaced a pilot system which was operational from May 2015 until March 2017, which contractors used to submit Excel based report templates to the SSRO. All data from the pilot system was securely migrated into DefCARS in March 2017.

Moving to a web-based application in March 2017 has improved the flexibility of the system and improved user experience and the ability to analyse data. Some changes to the data collected were also implemented in the transition to the new system. Changes were made to some reports to reduce duplication, and new fields were added to collect required information in a structured format.

DefCARS was moved from a private data centre into the public cloud, in the SSRO's Microsoft Azure environment (as per Annex A DefCARS Solution Overview) in 2022. This has enabled the SSRO to create a data warehouse (Synapse) with an associated ETL process to move data into this. The data warehouse then supports Power BI reporting to MOD and SSRO users.

[2] https://www.gov.uk/government/publications/ssro-defcars-future-technology-strategy

DefCARS future developments: The SSRO is considering work to replace the existing WebApp, and some of this work is expected to take place in the next contract period. This work is in the early stages, and could aim to replace a number of workarounds in the system, introduce efficiency gains including on how industry submits reports and system alignment to future legislation changes, and where possible look to resolve industry requests including improving user access flexibility which requires organisational hierarchies to be held within DefCARS.

DefCARS has around 2,500 active user accounts, 7,000 original and corrected report submissions and 2,000 – 2,5000 system log ins during a month. The DefCARS production database is currently around 40GB in size. The Synapse data warehouse is around 6GB in size.

Annex C: Specification requirements for core ITMS

IT Environment

The key deliverables required will be:

a) End user device, infrastructure, software, system and service configuration, administration, support, management and continuous improvement across the SSRO IT estate, except DefCARS and other third-party web applications which are out of scope (e.g. HR system, Finance system, digital Board and Committee system);
b) A Security Operations Centre as a Service, including cover for DefCARS. This must include the supply, deployment, and configuration of a Security Information and Events Management (SIEM) solution, with ongoing support, and 24/7/365 monitoring and events analysis, detection, and human response (including triage and analysis, containment, eradication, and recovery, as well as post-incident activities); and
c) Transition planning and transition for complete operational service including all onboarding activities for the Security Operations Centre.

These key deliverables are to be achieved through:

1. A full remote service desk, available 365/24/7, including fortnightly onsite support days. Service desk contact to include phone, email and chat function and meet SLA requirements for different incident priority classifications, including a security incident management process, as well as for resolution of VIP calls.
2. The supplier must hold and maintain ISO27001 and Cyber Essentials Plus certification as a minimum and hold and maintain relevant professional certifications for staff assigned to the contract such as Microsoft Competencies/Advanced Specialisms or GIAC Certifications. Service personnel must be SC/NPPV3 cleared.
3. The build and configuration of laptops / desktops (currently on Windows 11), iPads, iPhones and home printers, as well as identification of hardware faults and liaison with hardware suppliers (Dell and Microsoft). Management and configuration for all software installed on SSRO devices is required.
4. The provision of:
    - an enterprise architect to review and update our technology roadmap, including the provision of quarterly scheduled reviews;
    - a senior service delivery manager for day-to-day oversight and escalation of issues, including the provision of monthly service reviews;
    - a named contract manager to address commercial and contractual aspects of the ITMS/SOC contract and address systemic or longstanding service issues should any arise; and
    - a professional services capability to scope, quote for and implement change projects in addition to the ongoing operational service. This should include 12 days of resources of a mix of engineering, project management and service integration per quarter to meet the rolling continuous improvement programme, including security improvements as well as up to an additional 40 days per annum of a mix of engineering, project management and service integration for any such project, to be agreed and implemented following SSRO internal business cases and budget approval.
5. The management, administration, and support of the SSRO Azure tenant (core subscription) including security management (e.g. monitoring secure score and implementation of recommendations to maintain top quartile secure score) and

identity and access management. This includes Management, configuration and administration of Azure, Entra ID, Azure DevOps environment, Exchange, Office 365, SharePoint, Teams, Power BI, Servers and the DefCARS elements in Power BI and Azure DevOps (including liaison with the DefCARS supplier in respect of Secure Score reports and improvements of the DefCARS Azure subscription), as well as a proactive monitoring, alerting and response process across the estate.

6. The provision of service to fully manage, configure, administer, monitor, investigate and resolve any issues, and support the SSRO cloud-delivered Secure Access Service Edge ("SASE") architecture which provides secure internet access from any location with secure Wi-Fi connection to any application for all of SSRO end user devices.
7. A 365/24/7 Security Operations Centre as a service including protective monitoring and managed detection and response across the estate.
8. A service to administer, manage and support SSRO unified communications which is provided through Teams as a hosted service from Microsoft, including public switched telephone networks (PSTN) calling and Cloud private branch exchange (PBX).
9. The provision of a service to ensure that the SSRO M365/Azure/ZTA environment and associated supplier management assets are protected against viruses, Trojans, spyware, mass mailers, remote access toolkits, packers, potentially unwanted programs and all other types of malware.
10. The management and support for core common desktop services including fault finding, pro-active management of updates and advice around new versions. As a minimum this includes support for the M365 estate, SharePoint, Teams, Power BI, Azure information protection, exchange email.
11. The management and support for SSRO business applications. As a minimum this includes support for Sharegate and Azure Bastion.
12. The provision of robust physical security arrangements to protect all physical assets that store, process or manage SSRO data as well as security arrangements the SSRO M365/Azure/ZTA environment would rely on for maintaining the confidentiality of SSRO data to ensure controls are in place to protect it from unintentional access or unauthorised disclosure.
13. A backup and data retention, which must comply with Good Industry Practice and Standards as part of service take on. The following minimum service levels are required:
    - Backups are retained and restorable for at least three months.
    - The SSRO M365/Azure/ZTA environment including DefCARS must be backed up at daily (system and data) with the SSRO to approve the approach to full and incremental backup (e.g. weekly full and daily incremental).
    - The Supplier shall conduct routine backup and restore testing at least every six months to ensure that the backup and restore functions are functioning correctly. This can be conducted on a subset of backed up data and should be operated within representative, not production, environments.
14. The provision of a service to securely sanitise any SSRO data held by the Supplier when requested to do so by the SSRO, including securely destroying all Supplier media that has held SSRO data at the end-of-life.
15. Compliance with processes or plans for preparing for, and responding to, disasters or other service failures to maintain business continuity for the SSRO environment, which are reviewed and tested at least annually.

Annex D: Specification requirements for DefCARS

Overview of the DefCARS requirement

The SSRO's requirement is outlined in Table 1 and described more fully in the following sections.

Table 1: Outline requirement

Requirement	Description
Operational services	Provide operational services for DefCARS throughout the Contract Period, including application and data development, management and support.
Security	Meet the Security Requirements when delivering all aspects of the Contract, including the service design, the transition and transformation, and the provision of operational services.
Other matters	Meet the requirements for continuous improvement, quality, and conflicts.

The Supplier is not required to provide Microsoft licences and Azure services. The SSRO has an existing contract with a supplier (the "Reseller") for the provision of Microsoft (the "Cloud Platform Provider") licences and Azure services (the "Reseller Contract").

Operational Services

The SSRO requires operational services for DefCARS, including application and data development, management and support throughout the Contract Period, as described in Table 2.

Table 2: Operational services

Service requirement	Description
Carrying out Development Tasks	Undertaking Development Tasks, in-line with SSRO requirements and priorities, using DevOps methodologies. The need for Development Tasks may arise from many factors including: • SSRO required developments; • requirements to resolve Incidents and Bugs; and • changes to improve efficiency and security. A Development Task can change or relate to any aspect of DefCARS including the: • WebApp and application database; • Service design and configuration (including any associated documentation); • Database structure; • Overall security;

Service requirement	Description
	• Extract Transform and Load (ETL) processes; and • Reporting (MI reports to users).
On-going security management	On-going management of all security aspects of DefCARS including continuous vulnerability assessments and leveraging security monitoring services, in support of the assurance of DefCARS.
Working with third parties	Work with SSRO's third party suppliers involved in application development and support for the SSRO to ensure a coherent solution across the piece.
Production of management reports and monitoring	Monthly production of Service Delivery Reports including actuals vs agreed service levels and KPIs, with live information available based on the change control mechanism. Monthly updates to the Risk and Issues Log. Live operational performance reports including: • In liaison with the SSRO's ITMS/SOC supplier: WebApp downtime that is not due to hosting and the details; and Downtime that is due to hosting and the details. • User experience, based on system response times, for example for system login, report submission, uploading supplementary files and running analytics reports.
Backup and disaster recovery	Provide backup-as-a-service and disaster-recovery-as-a-service. Location and in-transit and at-rest protection of backups and recovery services must comply with the Security Requirements and must be agreed with the SSRO prior to service commencement.
Monitoring and event management	24x7x365 monitoring and event management of DefCARS that is not due to hosting.
Helpdesk[3]	Maintain email and telephone helpdesk support so that SSRO users may contact the Supplier in reference to Incidents and Bugs and other Development Tasks, and agree responses to these, to ensure swift resolution. A helpdesk offering support between 0900 – 1700 hours on each working day. • An out of hours contact for highest priority system Incidents or Bugs, including liaison with SSRO's ITMS/SOC suppliers as a result of proactive 24x7x365 monitoring being carried out by the ITMS/SOC supplier.

[3] The SSRO maintains its own helpdesk between 0900 and 1700 for defence contractors and MOD users to raise queries and issues relating to DefCARS. Issues are filtered and prioritised by the SSRO and will be raised by SSRO users with the Supplier where necessary.

Service requirement	Description
Change Control Mechanism	A complete incident, problem and change management service, including: • logging details about Incidents and Bugs and improvements to DefCARS; • identifying the source of Incidents or Bugs; • monitoring progress of dealing with system Incidents and Bugs and improvements and testing modifications to DefCARS; • code storage, versioning, and revision; • WebApp build, test and deploy through continuous integration and continuous deployment; and • sign-off by the SSRO of modifications prior to implementation.

In delivering DefCARS service support, the Supplier must implement and follow IT Service Management practises based on the ITIL v4 (formerly IT Infrastructure Library) framework or ISO 20000 standards.

The Change Control Mechanism is required to be the official log for all DefCARS related incidents, problems and change requests. A dashboard must be made available for SSRO staff to easily understand the status of Incidents and Bugs, in real-time. Where changes are progressed through the Implementation Plan and Testing Procedures, they shall also be included in the Change Control Mechanism.

The Change Control Mechanism is required to apply to DefCARS and shall interact with the following services and suppliers in the manner identified in the Final Service Design:

- the SSRO's ITMS and SOC and its supplier; and
- any Cloud Platform Security Centre and integration with Cloud Platform protective monitoring services.

The Change Control Mechanism shall include identifying the source of any Incident or Bug. The responsibility for meeting the cost of remedying the Incident or Bug is expected to be as set out in the second column of Table 3. The Supplier is required to submit a report to the SSRO identifying the source of each Incident or Bug within 10 working days. The SSRO will notify the Supplier in writing whether it agrees with the report findings within 10 working days. If the SSRO and the Supplier cannot agree the Source of an identified Incident or Bug, the question of responsibility for the cost of remedying the Incident or Bug may be referred to the dispute resolution procedure.

Table 3: Identifying the source of Incidents or Bugs and responsibility for remedying Incidents or Bugs

Source of the Incident or Bug	Responsibility for costs of remedying Incident or Bug
Work carried out by the Supplier (in service design, migration or subsequent phases)	The Supplier will meet the costs of making good the Incident or Bug without cost to the SSRO.
Problem with the cloud platform or underlying configurations within the remit of other parties (ITMS, Reseller or cloud provider)	The Supplier must liaise with the Reseller or ITMS supplier (whichever is appropriate) to understand and assist in resolving the matter, and the Supplier will agree in advance with the SSRO an amount of chargeable time it can incur in carrying this out based on the Day Rate.
Problem with an element of DefCARS in existence prior to the service going live with the Supplier	These will be treated as a Development Task.

As part of the Change Control Mechanism, the Supplier must ensure that Development Tasks, chargeable or otherwise, do not take place until formally agreed by the Buyer Representative or other authorised representative. The SSRO shall give notice in writing to the Supplier under the Contract of staff members who may act as authorised representatives for the purposes of authorising Development Tasks.

The SSRO will require Development Tasks to be carried out by the Supplier. Save where an alternative mechanism for commissioning Development Tasks has been agreed between the Parties, Development Tasks shall be commissioned by the SSRO through the Change Control Procedures.

The Supplier's proposed price of implementing the Development Task shall be calculated using a rate which shall in no event shall exceed the Day Rate and the number of days it is estimated in good faith that will be needed for carrying out the Development Task.

The Supplier shall prepare and submit to the SSRO the Impact Assessment within the time limit specified by the SSRO in the Change Form.

The Supplier shall ensure that the Development Task complies in every respect with the content of the Development Task Specification. In the event that Incidents and Bugs are identified, the Supplier shall remedy such Incidents and Bugs in accordance with Service Levels (and depending on Final Service Design) at its own cost. The Supplier shall maintain a detailed, itemised, up to date and accurate record of all time spent in carrying out each Development Task.

For the avoidance of doubt, the SSRO does not guarantee a minimum, or any, number of Development Tasks will be commissioned during the Contract Period.

Other

The Supplier will provide reusable libraries to assist with rapid development. The Supplier must also ensure that any development is in line with GDS best practice. The SSRO will:

- liaise with the Supplier to determine when the additional work within a period can be completed;

- carry out UAT on changes (unless it requests that the Supplier carry this out);

- gather feedback, including from the Supplier, on Development Tasks and prioritise these when reporting them to the Supplier, and may choose to alter priorities at any stage;

- inform the Supplier of any plans for Development Tasks in advance and agree with the Supplier when these can be implemented; and

- provide the Supplier with a Development Task Specification for the change required for each Development Task, to be agreed with the Supplier.

Security requirements

Security of DefCARS is a key priority for the SSRO. The Supplier must meet the Security Requirements when delivering all aspects of the Contract, including the design, migration, configuration, support and development of DefCARS. This includes:

- Accreditation and Assurance: security accreditation for handling information up to and including OFFICIAL SENSITIVE COMMERCIAL;
- System security: all information risks must be managed appropriately and that all necessary technical, physical, personnel and procedural controls are implemented by the Supplier against the identified risks. This includes all patching requirements;
- Certification Requirements: have and maintain certification throughout the Contract Period for Cyber Essentials PLUS and ISO27001:2013 / ISO27001:2022;
- Governance and Standards: The Supplier shall operate the DefCARS solution in consultation with the SSRO to ensure the security arrangements comply with the Security Requirements and the HMG, SSRO and MOD security practices;
- Personnel Vetting Requirements: All Supplier Personnel with Administrative level or regular access and Supplier Personnel with access to or working with live data must be subject to an elevated clearance level of Security Check (SC) or Non-Police Personnel Vetting Level 3 Checks;
- Physical Security: The Supplier must provide robust physical security arrangements to protect all physical assets that store, process or manage DefCARS data;
- Data Processing and Hosting: The Supplier must ensure that the physical locations where DefCARS data is stored, processed or managed do not prevent or hinder the accreditation and assurance of DefCARS;
- Protection of Information: The Supplier shall demonstrate and ensure that its (and other party's) security arrangements for maintaining the confidentiality of all DefCARS data are in place to protect it from unintentional access or unauthorised disclosure, manipulation or loss;
- Secure Data and System Transition and Migration: The Supplier must work with the SSRO and the out-going service provider as well as the ITMS/SOC supplier to plan and test the system and data migration including test scripts and data quality tests;
- User Groups, Permissions and Access Rights: The Supplier shall ensure that only approved users can access appropriately segregated data in the DefCARS Web Application, preventing unauthorised access to DefCARS functionality and information:

- Boundary Protection and Network Security: The Supplier must specify external firewalls and boundary protection services to protect DefCARS from attack and unauthorised access;
- Data-In-Transit and Data-At-Rest: The Supplier shall agree any data-in-transit or data-at-rest encryption mechanisms for the DefCARS solution during Service Design using NCSC configuration guidance and ensure that all DefCARS traffic operating over unprotected or untrusted networks is encrypted using Transport Layer Security (TLS1.2 or later as per NCSC guidance) configuration;
- Malware Protection: The Supplier must ensure that DefCARS and associated supplier management assets are protected against viruses, Trojans, spyware, mass mailers, remote access toolkits, packers, potentially unwanted programs and all other types of malware;
- Secure Management and Operational Security: The Supplier shall accept their security responsibilities for DefCARS system administration, management and configuration duties as communicated in the DefCARS Security Operating Procedures (SyOPs);
- Secure Design and Implementation: The Supplier must design and develop secure solutions and Cloud platform services in accordance with the NCSC Development and Deployment Guidance, NCSC Security Design Principles and NCSC Cloud Security Principles;
- Security in the Supply Chain: The Supplier must ensure that security in the supply chain is maintained for any sub-contracted services that may affect the DefCARS solution;
- Patching and Updates: The Supplier must ensure all necessary patches, updates and upgrades are applied in a reasonable time period to maintain supplier management infrastructure and devices;
- System and Data Backup: Any backed up data must be protected at all times. The Supplier shall document its approach to DefCARS backup and data retention, which must follow Good Industry Practice as part of Service Design;
- IT Health Checks: The Supplier must provision the services of an independent CHECK (refer to the National Cyber Security Centre (NCSC) website) or CREST (Council for Registered Ethical Security Testers) certified supplier to carry-out ITHCs, including penetration testing and security configuration reviews, against DefCARS before live implementation of any service;
- Protective Monitoring and Vulnerability Assessment: The Supplier must ensure an effective real-time protective monitoring and frequent vulnerability assessment regime is in place at all times;
- Security Incident Management: The Supplier shall provide the SSRO with its first response to any critical security incidents within one hour and initiate a co-ordinated incident investigation within two days and have out of hours support in the event of high priority incidents;
- Sanitisation and Disposal Requirements: The Supplier must securely sanitise any DefCARS information held by the Supplier when requested to do so by the SSRO, in case sensitive information needs to be removed or redacted; and
- Business Continuity and Disaster Recovery: The Supplier shall provide disaster recovery services, including requirements to assess failover arrangements The expected service level for a recovery point objective (the amount of data loss that is tolerable in the event of a disaster) is 24-hours.

Contract Management and Management Information

The Supplier shall ensure regular communication with the SSRO, and where necessary the SSRO's supplier of public cloud hosting for DefCARS and maintain a collaborative approach to maintenance and development. The Supplier must nominate a dedicated relationship manager to act as a key point of contact for the SSRO whose role is to:

- manage the service and relationship with the SSRO including the assignment of resources;
- ensure the quality and timelines of any deliverables;
- act as primary point of contact for the SSRO throughout the Contract Period;
- ensure compliance with Security Requirements;
- remain consistently informed about the Supplier's performance on all matters;
- be available to address Incidents or Bugs in a timely manner and meet any urgent requirements within an acceptable timeframe;
- ensure that the agreed price structure is followed and that costs are communicated to the SSRO on a routine basis throughout the service delivery; and
- be a point of contact for the SSRO's auditors if necessary.

The Supplier will provide management reports to support monthly service reviews and live operational performance reports. Monthly service update meetings shall be held between the SSRO and the Supplier, to discuss system operations, progress on Incidents and Bugs, plans for development work, risks and system security. The Supplier shall report monthly on actuals versus agreed service levels (as agreed in the Service Design), change control and the management of Incidents and Bugs based on information from the change control mechanism. A risk and issue log must be maintained detailing all identified risks and issues which may have an impact on the operation, development, security and delivery of DefCARS. Attendance at Contract Review meetings shall be at the Supplier's own expense.

Quality

The Supplier design and deployment must comply with Cloud Platform Provider technical standards and blueprints.

The Supplier must have a documented mature approach to quality management such as external code/configuration review processes as part of the system development lifecycle.

Conflicts of interest

The avoidance of Conflicts of Interest is critical to the SSRO.