7114498450
PROVISION OF ADS
SECURITY OPERATING CENTRE (SOC) SUPPORT

(DInfoCom/0260)

Statement of Requirement

CONTENTS

1. OUTCOME

1.1 The Army Digital Services (ADS) Security Operating Centre (SOC) Support will provide a cost effective, flexible and scalable cyber security support service that can meet the demands of ADS. Working alongside the existing in-house team, this support will provide the capability to continue the ongoing content and procedural development and cyber protection of ADS Army Digital Assets.

2. PURPOSE

2.0 The MoD may be referred to as “the Authority” hereafter.

2.1 The purpose of this document is to define the Security Operating Centre (SOC) Support services required by ADS. This is inclusive of, but not limited to:

2.1.1 On-going cyber protection of the AHE.

2.1.2 Development and upskilling of the existing in-house SOC team.

2.1.3 Use case development in line with existing, new and evolving cyber threats.

2.1.4 Log on-boarding so ensure adherence to Bulk Data controls and GPG13.

3. SOR COMPOSITION

3.0 This document is split into three schedules:

3.0.1 Schedule 1 - Background to the ADS Organisation.

3.0.2 Schedule 2 - The Services required.

3.0.3 Schedule 3 - The Service levels required.

4. HARDWARE AND SOFTWARE INFRASTRUCTURE PROCUREMENT

4.0 The Authority will be responsible for procurement of all the IT assets and equipment required to support this requirement.

5. INTELLECTUAL PROPERTY RIGHTS (IPR)

5.0 The selected Supplier shall not retain IPR relating to any services delivered during the terms of the contract.

6. LICENCING AND SUPPORT AGREEMENTS

6.0 The Authority will retain the overall responsibility for ensuring that all system software utilised by the Service Supplier on behalf of the Authority is fully licenced with the provider.

7. EXIT PLAN

7.0 The Authority and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier Deliverables to be transferred to the Authority ensuring that the Authority has all the documentation required to support and continuously develop the Service with Authority resource or any third party as the Authority requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work (SoW) may be agreed between the Authority and the Supplier to specifically cover the exit plan.

8. DURATION

8.0 The duration of the overall requirement is for a twenty-one (21) month period, from 01 Nov 2024 until 31 Jul 2026, with a twelve (12) month option period.

SCHEDULE 1 – BACKGROUND TO THE ADS ORGANISATION

9. OVERVIEW

9.0 This following section is designed to provide information, for context, on the structure, organisation, processes and remit of the Authority. It is therefore broader than the specific needs of this contract which are detailing in the following schedules.

9.1 ADS provides hosting and through life application-based information services to the Army and wider Defence; predominantly through web applications accessible either on the intranet or on Defence infrastructure. It comprises of a core of 100+ personnel across military, Civil Servants (CS) and core Technical Support staff which includes elements from 605 Signal Troop (13 Signal Regiment) that directly support ADS. This figure increases when new products are in delivery.

9.2 ADS provides hosting capability across three security domains in the form of Official, Official Sensitive and Secret. The official domain is provided by the Defence Gateway(DGW) capability and is currently provided under a MoDCloud contract. In the Official-Sensitive and Secret environments, ADS provides the hosting platform (hardware and software) in the form of a private cloud; known as the Army Hosting Environment (AHE). The landscape of ADS hosting capability is as detailed on Page 6, Figure 1. In addition to these hosting capabilities, some aspects of the pipeline for delivery onto both the DGW and AHE are in Microsoft Azure, enabling remote access to the product teams.

10. THE ARMY HOSTING ENVIRONMENT (AHE)

10.1 The AHE is a 'private cloud' located on MOD premises that currently supports 70+ business applications across multiple security classifications. In the Official-Sensitive and Secret environments, this is connected to the military WAN. ADS provides the hosting platform in the form of a fully Software Defined Data Centre (SDDC) (using VMware technology) to enable applications to be accessed from a web browser on MODNET at Official-Sensitive and Secret.

10.2 The applications hosted on AHE support a wide range of functions across HR, logistics, intelligence, finance, command, and control. These include several applications that have been developed by ADS on behalf of the Field Army, the more significant ones of which include:

10.2.1 CHURCHILL - an event scheduling application;

10.2.2 OPUS - a single tasking mechanism;

10.2.3 MUSTER - a personnel deployability tool;

10.2.4 MARSHAL - an equipment availability tool;

10.2.5 Reserve Attendance and Pay Service - a Reserve Army management system;

10.2.6 TARGET - an individual training management system; and

10.2.7 MyMUSTER - a system which reports on individual readiness to soldiers.

10.3 More broadly there are currently 70+ live application services on the Official-Sensitive, of which 25+ are Oracle APEX, 8 are .Net; 2 utilising Software AG technology and the remainder are Commercial Off the Shelf (COTS). The COTS products include Microsoft

Customer Relationship Management (CRM) Dynamics, SharePoint and Remedy which are configured

to meet the requirements of the users. Other COTS products are used in the form of ResourceLink to pay civilian employees in the Army.

10.4 The Army also has a significant Management Information (MI) and Business Information (BI) capability in the form of the Army Data Warehouse (ADW) utilising Oracle Business Intelligence Enterprise Edition (OBIEE) and Statistical Analysis Software (SAS) ViYa, to provide reporting and analytics across the Army. On Secret, there are 6 application services. This is anticipated to grow due to the lack of Secret hosting facilities across Defence.

10.5 Application users range from a handful for some of the more specialist applications to tens of thousands for those widely used across the Army and pan Defence, including the RAF, Navy and Defence Equipment & Support (DE&S).

10.6 ADS is now moving to an Application Programming Interface (API) first strategy based on services from the system of records mediated through an API Gateway. As applications are being improved or delivered the opportunity is being taken to break down existing applications into their component parts and delivered as business services.

10.7 ADS are also looking into the use of public cloud to include VMC on AWS with a view to deliver a Hybrid Cloud allowing centralised management and interoperability between applications and services that bridge security domains.

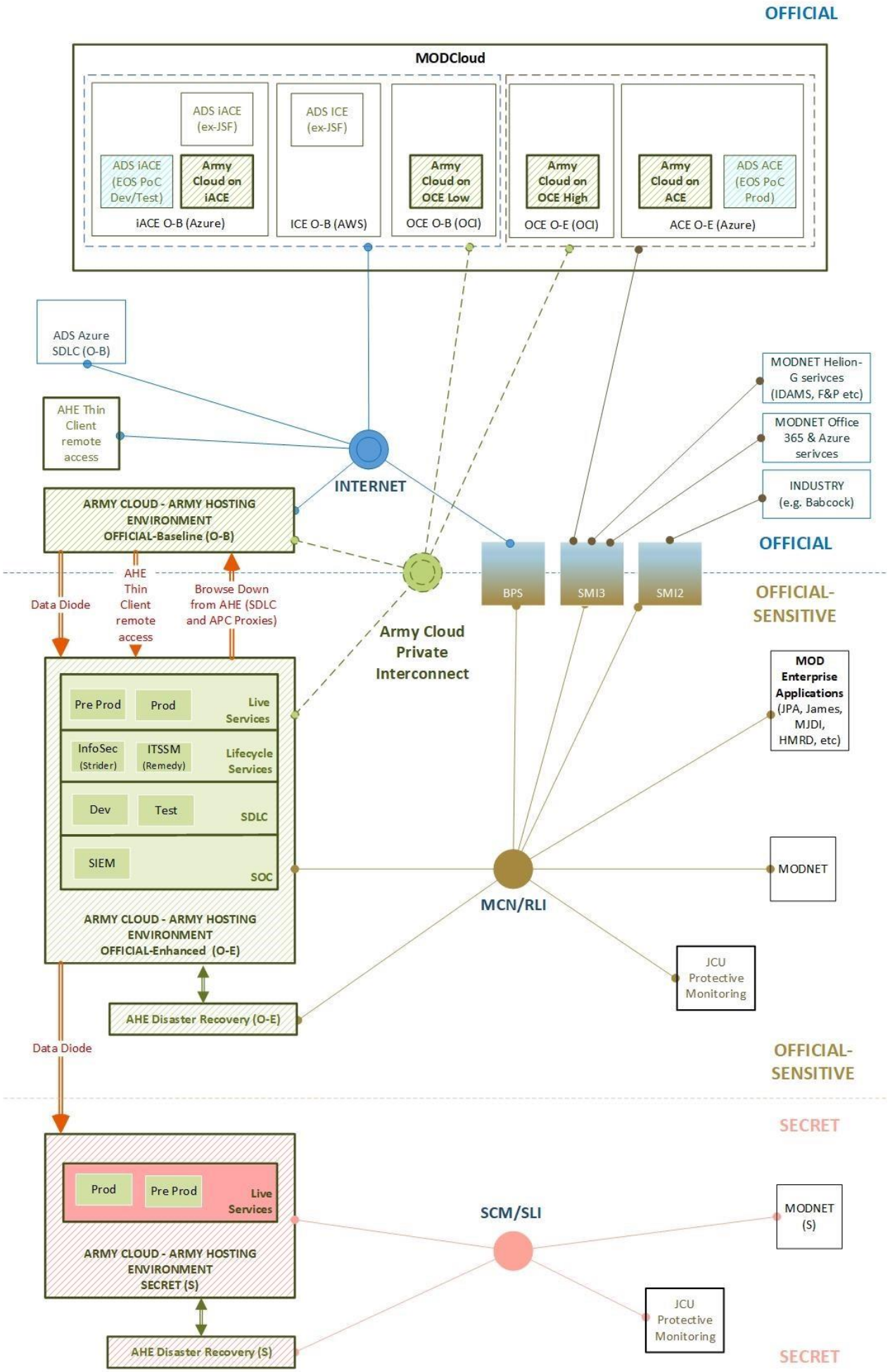

OFFICIAL
MODCloud
ADS iACE (ex-JSF)
ADS ICE (ex-JSF)
ADS iACE (EOS PoC Dev/Test)
Army Cloud on iACE
Army Cloud on OCE Low
Army Cloud on OCE High
Army Cloud on ACE
ADS ACE (EOS PoC Prod)
iACE O-B (Azure)
ICE O-B (AWS)
OCE O-B (OCI)
OCE O-E (OCI)
ACE O-E (Azure)
ADS Azure SDLC (O-B)
AHE Thin Client remote access
INTERNET
MODNET Helion-G serivces (IDAMS, F&P etc)
MODNET Office 365 & Azure serivces
INDUSTRY (e.g. Babcock)
ARMY CLOUD - ARMY HOSTING ENVIRONMENT OFFICIAL-Baseline (O-B)
OFFICIAL
Data Diode
AHE Thin Client remote access
Browse Down from AHE (SDLC and APC Proxies)
BPS
SMI3
SMI2
OFFICIAL-SENSITIVE
Army Cloud Private Interconnect
MOD Enterprise Applications (JPA, James, MJDI, HMRD, etc)
Pre Prod
Prod
Live Services
InfoSec (Strider)
ITSSM (Remedy)
Lifecycle Services
Dev
Test
SDLC
SIEM
SOC
MODNET
MCN/RLI
ARMY CLOUD - ARMY HOSTING ENVIRONMENT OFFICIAL-Enhanced (O-E)
JCU Protective Monitoring
AHE Disaster Recovery (O-E)
Data Diode
OFFICIAL-SENSITIVE
SECRET
Prod
Pre Prod
Live Services
SCM/SLI
MODNET (S)
ARMY CLOUD - ARMY HOSTING ENVIRONMENT SECRET (S)
JCU Protective Monitoring
AHE Disaster Recovery (S)
SECRET

Figure 1 – AHE Landscape

11. DEFENCE GATEWAY (DGW)

11.1 The DGW provides an official capability that is accessed via Single Sign On (SSO) behind which there are currently 26 services of which 7 are ADS delivered. These are predominantly web services with a handful of native mobile applications. The web services provided range from COTS, in the form of web e-mail, SharePoint (used as a Content Management System) and Jive (known as Defence Connect). The bespoke developed services include, a portal page (consolidating access to all the services), MoDBox (an MoD variant of DropBox) and Reserve Attendance & Pay Service (RAPS) and My Admin (provides pay statements). The remainder of the services/application are third party provided utilising Platform as a Service (PaaS) and the DGW SSO.

12. OPERATING MODEL

12.1 ADS has invested significant time and effort to adopt Agile and then start to mature as a DevSecOps organisation. A pipeline approach has been established for deploying onto both the AHE and the DGW, utilising the same technologies for the majority.

12.2 The product teams are utilising Continuous Integration (CI) and Continuous Deployment (CD) with SCRUM as the agile framework. The in-service team have adopted Kanban. A Significant and on-going investment has been made to automate testing.

12.3 The Service Operations and Management teams utilise ITIL for change, incident, problem, knowledge and asset management. Remedy is used as the main IT Service Management Tool. The change and incident processes are used to capture the requirement but are then fed into the DevSecOps ways of working.

12.4 The Service landscape on AHE is as detailed below in Figure 2.

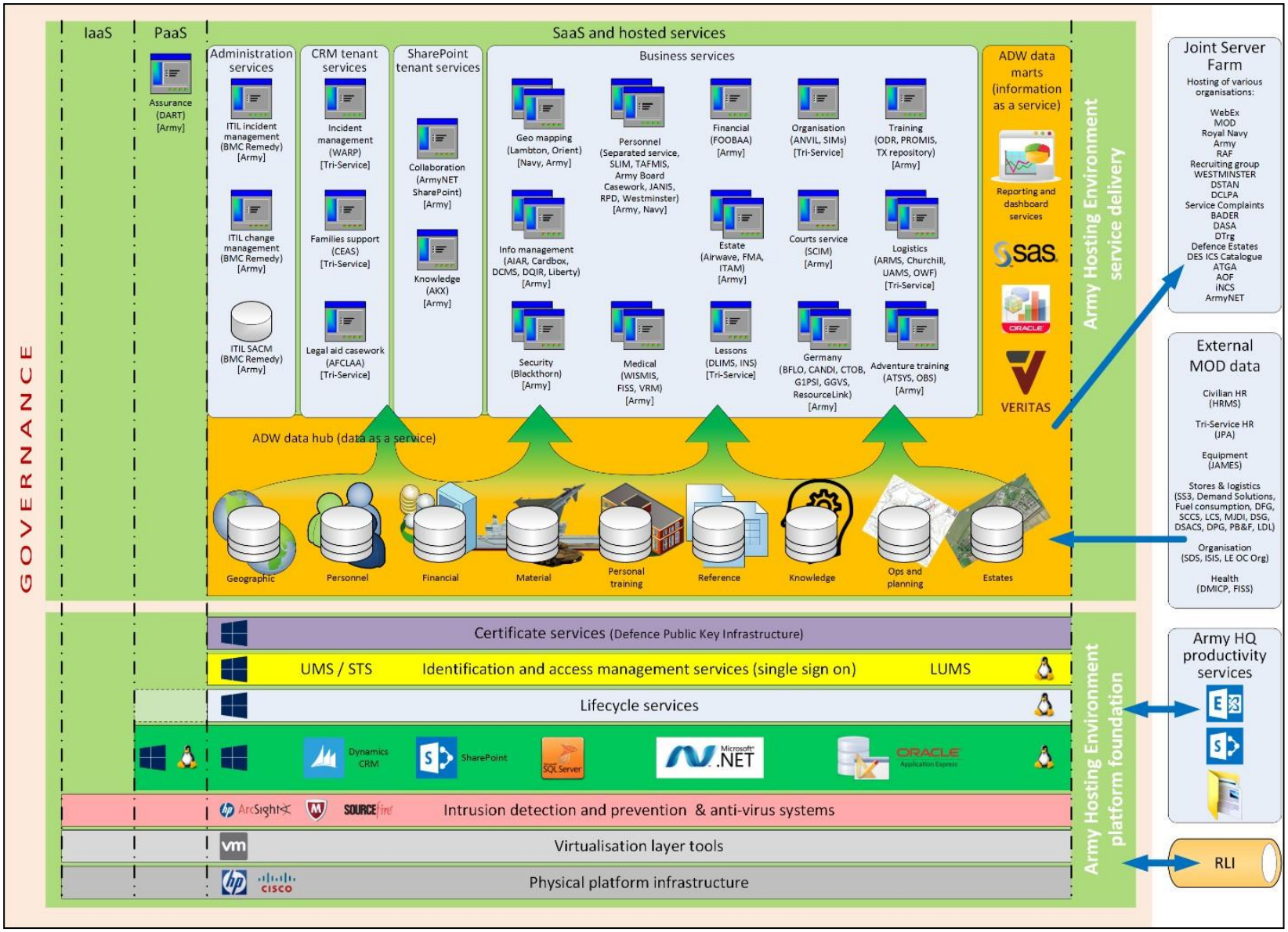
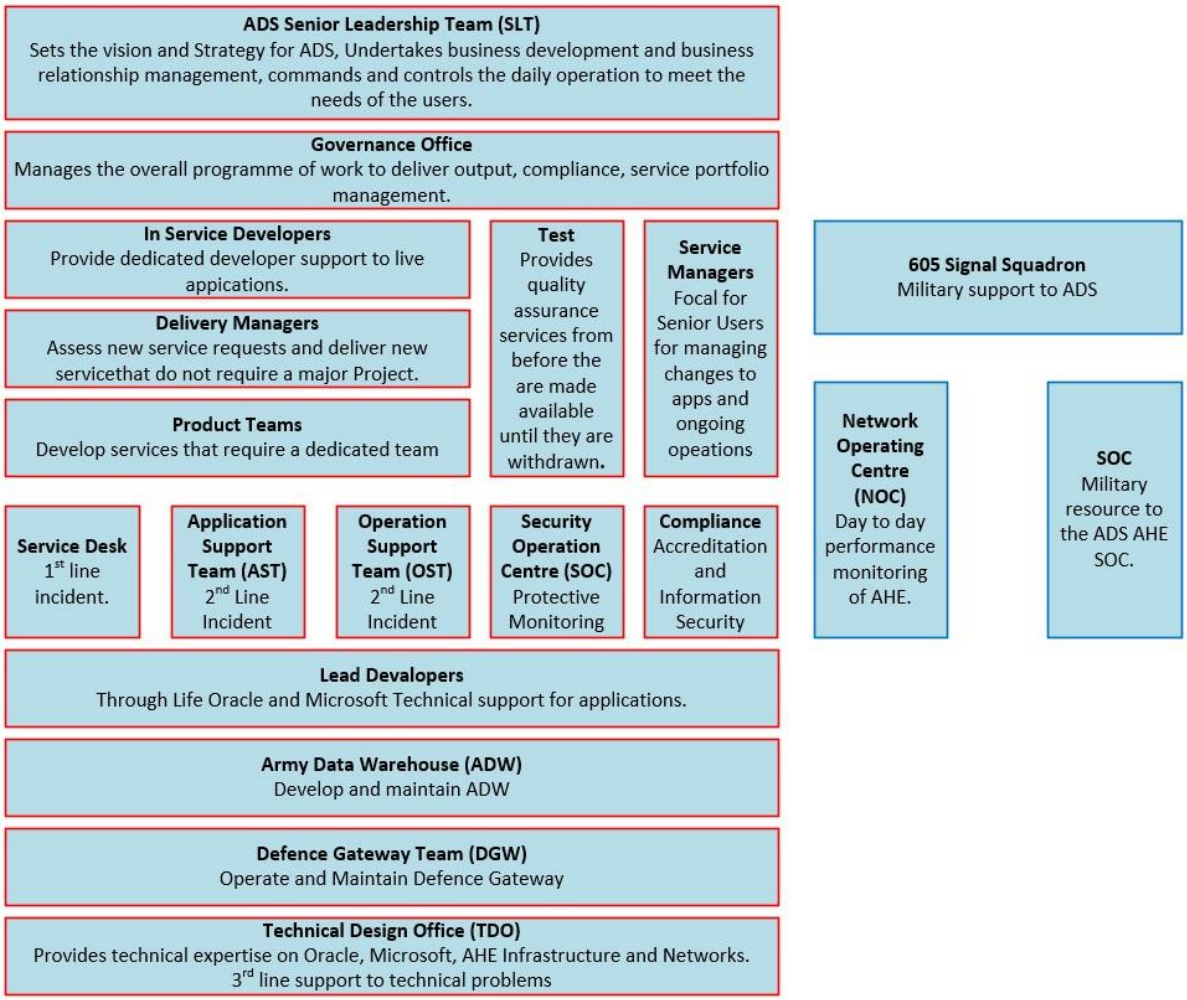


Figure 2 _ Service landscape on AHE

13. ADS ORGANISATION, ROLES AND RESPONSIBILITIES

13.1 The structure of ADS and 605 Signal Troop is detailed in the diagram below and in the following paragraphs:



13.1.1 **Product Teams.** These are based predominantly on a 4-6 resource team, comprising of 2-4 developers, 1-2 testers, and a Business Analyst (BA) as their primary skills but all are multi-disciplined. These teams use SCRUM as their main framework for delivering software.

13.1.2 **In-Service Development Team.** These consist of 3 Oracle APEX and 2 .Net Developers with 3 testers matrix managed to enable the Service Managers to make changes to the services they support. These work on bug fixes and minor changes to live services. As the code base is changed the automated scripts are updated. Kanban is the agile framework used to process work. The Service Development Team also provide 3rd line support for the resolution of incidents and problems with application services. ADS has the ability to provide remote Dev/Test for this team utilising Azure. The main Dev/Test is on AHE v2 with automated release on to production.

13.1.3 **Test.** ADS has shifted left with testers imbedded in the product and inservice management teams. These testers are responsible for the automation of the functionality and regression testing. As part of the CI pipeline, after Dev/Test the next phase is System Integration Testing (SIT), where the software is tested on as close to production environment as possible; on SIT integration and exploratory testing are conducted; as well as the assurance of the automation tests. The technical assurance is provided by a senior tester.

13.1.4 **Army Data Warehouse (ADW).** The ADW is the single repository for the consolidation of Army and Defence data, which is then used to enable reporting on Army activities. The ADW is also the hub for integration of other ADS applications and services ensuring use authoritative data.

13.1.5 **Defence Gateway Team.** This is a small DevSecOps team that does everything from supporting the infrastructure, to developing new services and maintaining them on the Defence Gateway (internet – official). Services include MoDBox (drop box equivalent), SharePoint, e-mail, Defence Connect (Jive) and applications to support activities such as Reserve Pay. The team has normally undertaken its own testing but has recently had a tester embedded to follow the same operating model as the rest of ADS with a pipeline of environments and automated testing. At present a single tester has been dedicated to this team. The DGW team utilise Azure for their Dev Test and Pre-production with production currently being delivered via MoDCloud.

13.1.6 **Operation Support Team (OST).** 2nd line network and infrastructure management.

13.1.7 **Network Operation Centre (NOC).** A team of predominantly military (from 605 Troop) and civil servants with some Technical Support contractors. This team supports the AHE v2 for the Official Sensitive and Secret Environments. Responsibilities include support and maintenance of the storage, network, compute, hardware VMware tech stack (including virtualised network), VMs, OS and monitoring the health of applications/services. For all technical matters they are supported and guided by the TDO.

13.1.8 **Service Desk.** A team of civil servants and military that provide the first line of support for applications. This Service Management as a Service requirement will work alongside this in-house capability.

13.1.9 **Service Management.** A team of civil servants and military that ensure that applications continue to satisfy the evolving needs of the business and to support their Business-as-Usual. This Service Management as a Service requirement will work alongside this in-house capability.

13.1.10 **Application Support Team (AST).** This a team of mainly Civil Servants with technical support contractors. The main role of the team has been

the transition of services onto Pre-Production and Production and provide

second line support for application incidents and problems. The transition of services is now being automated utilising Microsoft Release Manager.

13.1.11 **Technical Design Office (TDO).** This is the main technical hub of the organisation, with the technical expertise for all the technologies employed by ADS. They are responsible for deploying new infrastructure services, handing over knowledge to the relative teams and providing 3rd line support for these services, predominately infrastructure and main core services for the data centres.

13.1.12 **Delivery Managers.** The delivery of new or small to medium sized services within ADS is the responsibility of Delivery Managers; this could be anything from an infrastructure change to a small product/service.

13.1.13 **Compliance Team.** Provides in-house advice to ensure ADS adheres to security and policies as laid out in Joint Service Publication (JSP) 440 and 604, ISO 27001 and security architecture. AHE Security Accreditation Coordinator (SAC).

13.1.14 **Configuration Team.** Responsible for the configuration control of hardware, software and documentation.

13.1.15 **Security Operations Centre.** Responsible for the protective monitoring of the AHE (O & S). Defensive Cyber Operations (DCO).

13.1.16 **Army Data Analytics.** The Army Data Analytics Team offer a range of analytical services to enable the business to gain insight and benefit from enterprise data. Dashboards display data visualisations of the current and historical status of metrics and key performance indicators for the enterprise.

13.1.17 **Land System Reference Centre (LSRC) Services**. The LSRC provides a service enabling System of Systems integration in support of Operations, and major capability development programmes. The service provided includes connectivity, tooling, application and service expertise, and skills to operate the service in a multi mission configurable environment.

SCHEDULE 2 – SERVICES REQUIRED

14. OVERVIEW OF REQUIREMENT

14.1 To enable conformity to Cyber Defence and Risk (CyDR) security accreditation agreements for the Army Hosting Environment (AHE). ADS has established a Security Operating Centre (SOC) to monitor and detect real-time activity on the AHE to protect against internal and external security threats. Work is ongoing to ensure the SOC can effectively monitor the (OS), (S), (O) and SDLC environments to ensure the SOC remains compliant with CyDR.

14.2 The requirement broadly falls into two parts. 24/7 Protective Monitoring and Support, Development and Maturation of the AHE SOC.

14.3 To provide the necessary technical Suitably, Qualified, Experienced, People (SQEP) resource to deliver Authority-defined outcomes that will include Defensive Cyber Operations (DCO) Protective monitoring (PM) as part of a 24/7 shift pattern.

The supplier will need to have adequate resource available to deliver the Statement of Work (SoW) deliverables. Protective Monitoring will include the resource to provide service for all bank holidays (including Christmas). Resources will need to be SQEP, familiar with AHE SOC processes and have been ‘on boarded’ onto AHE and Army HQ.

14.4 To provide the necessary technical SQEP resource to deliver Authority-defined outcomes that will include but are not limited to; developing the AHE SOC maturity , developing Cyber Security Incident Management and Response (SIMP) plan, Review and develop on-boarding process and procedure for IaaS, PaaS and SaaS, Use Case and content creation and training and development of the existing SOC team. The service needs to be undertaken by technical outputs who hold MOD Security Clearance (SC) as a minimum, with a strong technical background and a very good understanding of industry and defence Cyber Security compliance policy and practices.

To provide Advice, guidance, and technical recommendation to develop the AHE SOC to an industry level best practice standard.

14.5 The supplier will need to have the resource capacity to deliver service in the event of a regular resource requiring absence for DCO PM. E.g. Planned absence such as leave and unplanned leave caused by illness or other unforeseen circumstances.

14.6 The Supplier will be required to provide a client interface to agree business prioritisations and deliverables.

15. DELIVERABLES

The high-level deliverables for the service are outcomes associated with

15.1 Defensive Cyber Operations (DCO) Protective Monitoring (PM) SOC Analysts (SFIA level 4) deliver DCO PM as part of a 24/7 Shift Pattern. This forms part of a whole force DCO PM approach.

1st Line security incident triage and reporting and typical associated SOC Level 1 protective monitoring duties.

DCO PM 24/7 shift pattern. Typically, 46 shifts/month (up to 62 shifts a month), depending on the days per month. Currently each shift is 12 hours. Day 07:00 to 19:00. Night 19:00 to 07:00. This may change with consultation with supplier.

Protective monitoring will include all bank holidays (including Christmas). Resources will need to be familiar with AHE SOC processes and have been 'on boarded' onto AHE and ARMY HQ.

Support and training to existing AHE SOC Analysts.

Any additional other support or development tasks required by SOC Manager or ADS Senior Leadership Team (SLT) within the scope of AHE SOC.

15.2 AHE SOC Support, Development and Maturation (SFIA Level 5) deliverables include but are not limited to:

Act as a focal point for Security Incident escalation. A focal point for advice guidance, support and, if necessary, action on Security Incidents raised and typical associated SOC Level 2 duties.

Support 1st line analyst triage and escalation.

Build/Develop Use Cases – Develop use case and facilitation, threat modelling and translation of operational requirements into SOC SIEM tool. Focus on insider threat and Data Loss Prevention use case to demonstrate the process used by SOC analysts.

Cyber Security Incident Management Plan (SIMP). Develop the AHE Cyber Incident Response Plan in line with NIST and SANS guidance and incorporating the wider ADS teams. Create supporting documentation and guidance for SOC and ADS to follow OOH with clear lines to resolver group support.

SOC Roadmap development – assist in Developing SOC in line with recommendations, from the ADS Security Architect, industry Best Practices and ongoing AHE SOC Security Operations Maturity Assessment (SOMA).

IaaS, PaaS and SaaS On-boarding – Work with wider development teams and develop, process for log on-boarding and develop costing model for SOC.

Official ‘O’ and Software Design Life Cycle ‘SDLC’ scope out – Review of network diagrams of both environments and prioritise log on-boarding into the SOC SIEM tool. Breakdown of workable project sizes and raise CRQ’s with dependant teams for on boarding.

Develop SOC BCDR – Review existing documentation for the SOC BCDR and ADS/ HQ and develop process/plan that feeds into the wider process.

Cyber Incident Investigation/Escalation – Reviewing event channel and MoDCERT and identifying issues for escalation to different teams in ADS.

Training and development – Mentor existing SOC team and develop play books and training and development content to enable quick upskilling of new starters to the SOC.

Any additional other support or development tasks required by SOC Manager or ADS Senior Leadership Team (SLT) within the scope of AHE SOC.

It is expected that AHE SOC Support, Development and Maturation can be delivered within Business Working Hours (BWH) but may need to be delivered out of BWH in line with ADS Business Requirements.

16. ESSENTIAL SKILLS AND EXPERIENCE

16.1 DCO Protective Monitoring, SFIA Level 4:

Overall, the Authority’s requirement is for outcomes likely to be delivered by skilled resource and the following details the skills and experience which are mandatory to ensure the Supplier can meet the Authority’s current and potential future requirements for this requirement:

Strong knowledge Cyber Security, with a focus on operational security. Such as security monitoring and alerting, vulnerability management and incident response. Producing supporting security documentation in coordination with stakeholders.

A good all-round knowledge of IT systems and Networking.

Experienced in both updating and creating operational security processes and procedures.

Comprehensive experience of working in Security Operations Centres (SOC), with additional knowledge and experience to support junior colleagues within the SOC.

Effective communication skills being able to deliver technical conversations and presentations to a range of different stakeholders.

Network and application security and architecture, incident response, forensic investigation, and business continuity management.

Knowledge of various Cyber Security Frameworks, Data Protection, and bulk data controls.

Hands on experience with security tooling such as SIEM and EDR solutions. Technical ability to operate them from both an analyst and engineering perspective. (Monitoring, Use Case and content creation, upgrades, and troubleshooting).

Ability to monitor, assess, triage, escalate alerts and incidents detected on the SEIM.

It is desirable that resources have current working knowledge of MoD systems and networks and have evidence of previously providing services to MoD or security services.

16.2 AHE SOC Support, Development and Maturation, SFIA level 5 Technical Cyber Security and Security Administration Subject Matter Expert (SME).

Overall, the Authority's requirement is for outcomes likely to be delivered by poly-skilled resource and the following details the skills and experience which are mandatory to ensure the Supplier can meet the Authority's current and potential future requirements for this requirement:

Strong knowledge Cyber Security, with a focus on operational security. Such as security monitoring and alerting, vulnerability management and incident response. Producing supporting security documentation in coordination with stakeholders.

A good all-round knowledge of IT systems and Networking.

Experienced in both updating and creating operational security processes and procedures.

Comprehensive experience of working in Cyber Security Operations Centres (CSOC), with additional knowledge and experience to support junior colleagues within the AHE SOC.

Effective communication skills being able to deliver technical conversations and presentations to a range of different stakeholders.

Network and application security and architecture, incident response, forensic investigation, and business continuity management.

Knowledge of various Cyber Security Frameworks, Data Protection, and bulk data controls.

Hands on experience with security tooling such as SIEM and EDR solutions. Technical ability to operate them from both an analyst and engineering perspective. (Monitoring, Use Case and content creation, upgrades and troubleshooting.

Ideally have professional certification such as GIAC GCIH, CISSP, CISM or ISO 27001.

Experience working in a Defence environment.

Experience of managing and/or mentoring technical personnel.

Knowledge of on-boarding new log sources into a SOC for security monitoring, while exploring relevant Use Cases for the respective log sources.
Where requested the Supplier would be expected to justify SFIA levels of resources utilised in this work in terms of professional memberships, training, qualifications, certifications and above all examples of prior work and experience that is relevant to the role(s) they are assigned against.

The Supplier and the resources it provide must be free of any commercial ties or obligations to any hardware or software vendors.

It is desirable that resources have current working knowledge of MoD systems and networks and have evidence of previously providing services to MoD or security services.

17. LOCATION

17.1 The normal place of work for this requirement is Army HQ (AHQ), Marlborough Lines, Andover, Hampshire, United Kingdom. Although a proportion of this work will be suitable for remote working, under an agile approach there will be routine occasions where team collaboration is essential, as is engagement with the user community, and ADS departments. All Secret Network access has to be conducted at AHQ, Andover. As such it is not considered to be appropriate that this requirement is satisfied by offshore resources working outside the U.K.

18. SCALING

18.1 The ability for the Authority to scale up or down rapidly is a key requirement in order to respond to the dynamic needs of ADS, including the ability to resource urgent operational requirements. As such, and subject to demand and budget, the Authority requires the ability to scale up and down the resource requirements in relation to outputs. In essence, this means that there will be a minimum (core) level below which the quantity of outputs will not fall and beyond this a discretionary level that the Authority may choose to exploit in part or whole at various stages throughout the contract.

18.2 The requirement for change in outputs would take 2 forms:

18.2.1 **Additional Outputs (expansion)** - if an initiative requires a new/further set of skills. For example, a new application is developed for which the

outputs commensurately require a new Security Assurance Co-ordinator capability to be established. This would be over and above the current 'on-going' outputs and resource provision. or,

18.2.2 **Re-prioritisation of Outputs** - if there is need to pivot outputs in response to the Authority's demands which may require a different skill-set. For example, as the expansion of a particular application evolves there is a need to re-focus outputs.

18.3 The Authority will require confirmed rate cards for the provision of resources to deliver new work. This would involve the ability to select pre-defined service offerings in relation to new outputs that would be above the core service. Due to budgetary constraints it is envisaged that the service would be on a capped T&M basis that would enable the Supplier to confirm a maximum cost to meet the outputs required over a set period.

18.4 Although the requirement will not fall below the minimum level of the contract the Authority may also require discontinuing of certain activity at its discretion which in turn may lead to exit (off-boarding) of certain resources.

SCHEDULE 3 – SERVICE Levels

19. PROVISIONING

19.1 The Service Supplier will be the main point of contact with the Authority.

19.2 The Service Supplier is expected to ensure delivery of Resource requirement.

19.2.1 Provision of further resources within twenty-five (25) calendar days.

19.2.2 Exit of current resources no longer required within seven (7) calendar days.

20. SECURITY REQUIREMENTS

20.1 All outputs that fulfil this requirement will need to have a minimum level of Security Clearance and be subject to vetting. The minimum standard is MOD Security Clearance (SC), although on occasion the Authority may prescribe a higher level of Security Clearance. This will be applied on a case-by-case basis to both existing and new resources where the Authority has the requirement to do so. The Service Supplier warrants that all staff used to supply their service hold current, MOD applicable, Security Clearances at SC level or above and are willing and eligible to obtain higher clearance levels if the role requires it.

21. CONTINUOUS IMPROVEMENT

21.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

21.2 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.