# ARMY DIGITAL SERVICES
# TECHNICAL DESIGN OFFICE
# STATEMENT OF REQUIREMENT

| | |
|---|---|
| Project Name: | Technical Cloud Architecture Design, Security and Support (TCADSS) services |
| Document Release: | **Final** |
| Version Number: | **1.7** |
| Date: | **21 Nov 25** |

| | |
|---|---|
| Author: | **Lt Col R Hill** |
| Project Executive: | **Col J Dagless** |
| File Number: | **715728453 (DInfoCom/0318)** |
| SharePoint URL: | |

**Introduction**

Army Digital Services (ADS) wishes to contract a supplier to provide a comprehensive Technical Cloud Architecture Design, Security and Support (TCADSS) Service. The service will be delivered as an outcome-focused, self-managed capability that assures, designs, delivers, and evolves the ADS Army Cloud and related platforms.

**In summary (detailed in Schedule 1), the service will provide:**

- Technical Cloud Support Service to deliver ADS Army Cloud initiatives, ensuring provision, management, support, and exploitation of the Army Cloud across public, private, and hybrid cloud environments.
- A Technical Design Office (TDO) Service, acting as the through-life design authority for all ADS-owned systems and services. This will deliver Solution, Security, System, and Platform Architecture functions, ensuring alignment to Enterprise Architecture while providing ongoing assurance, governance, and roadmaps.
- Platform Engineering functions spanning the full development lifecycle, including environment provisioning, CI/CD integration, automation, resilience engineering, and 4th line incident escalation.
- Deployable and Land Systems support, designing and delivering mission-ready, secure, and resilient deployable services for tactical and contested environments.

- Cost Modelling & Compliance Functions, including through-life cost modelling for cloud hosting and design services, Software Asset Management (SAM) design and approach for licence compliance, and platform compliance assessments.
- Security Operations Support, including the design and infrastructure management of the ADS SIEM solution, ensuring integration with the SOC and Land mission systems.
- Enterprise Architecture Tools Management, ensuring ADS architecture artefacts, models, and reference patterns are maintained and integrated within a central repository.
- Innovation & Emerging Technology Advisory, including horizon scanning, R&D proof-of-concepts, and AI initiatives, ensuring ADS can adopt, trial, and exploit new technologies securely and effectively.

**Typical Scenarios to be Supported (non-exhaustive):**

- **Cloud Hosting** – manage the current public / private / hybrid clouds to ensure a secure infrastructure. Manage capacity and availability.
- **Platforms** – design, build and operate platforms suitable for hosting bespoke and COTS applications, needed by ADS customers, both at OS and S.
- **Network Management** – manage hardware and software-based networking (e.g. firewalls) to ensure that the Army products and services retain a secure perimeter and an internal zero trust network model. Ensure that the networking infrastructure is patched and updated to eliminate obsolescence and manage any compliance risks.
- **Incident Management** – support the management of services affecting incidents within the portfolio, responding to these in the timeframe of the ADS SLA.
- **Monitoring & SIEM** – ensure that the relevant logging and alerts from ADS-owned infrastructure and solutions are passed to the ADS Security Operations Centre (SOC). Design, deliver, and manage the SIEM platform as part of the service.
- **Infrastructure Management** – regularly review and upgrade the private element of the Army Cloud hardware (compute, storage etc.) and the software-defined data centre stack to maintain a highly available system.
- **Systems Administration** – support the physical and virtual infrastructure. Provide 3rd and 4th line support of issues. Draft and maintain appropriate security policies to control access based on least-privileged models.
- **Continuous Integration / Continuous Development** – support the CI/CD pipeline by deploying the relevant tools, on premise and within MoDCloud (AWS, Azure, Oracle) into the appropriate production environments.
- **Design and Verification** – provide designs, migration strategies, and assurance artefacts to deliver the defined outcomes for ADS.
- **Technology Roadmap** – deliver and maintain the ADS technology roadmap, including through-life cost modelling and compliance considerations.
- **Security Architecture** –
    - Conduct security **risk assessments** and threat modelling for systems and services.
    - Provide **Risk Advisory Notes** and security design guidance to ADS leadership.
    - Deliver and maintain **security reference models, reusable patterns, and control frameworks**.
    - Support **accreditation and assurance** activities with required artefacts.
    - Provide **expert advice and guidance** on emerging security risks and mitigation strategies.
    - Conduct **post-incident analysis** and recommend design improvements.
- **Deployable and Operational Systems** – design, assure, and support deployable and mission-ready platforms for use in military operational land systems context.
- **Software Asset Management (SAM) & Compliance** – deliver licence compliance, optimisation, and platform compliance reporting.
- **Emerging Technologies, R&D & AI** – conduct horizon scanning, deliver proofs-of-concept, and provide CTO advisory reports on adoption of new technologies and AI-enabled solutions.

ADS expects to contract the supplier to provide a suite of fully self-managing services (ADS refers to these as ‘as a service’ capabilities):

All work items to be actioned by this service will be processed via the organisations Information Technology Service Management (ITSM) and Information Security Management System (ISMS).

ADS does not wish to be involved in the planning and implementation of the delivery of these services, noting for incident resolution there are central SLA timeframes the service will need to adhere too.

ADS will only be responsible for the assignment of business priorities to the service deliverables. (e.g. 'platform A is required before platform B') and advising timeframes for completion.

As ADS does not, as above, understand the complexity and technology involved in delivering the IT services, ADS expects the supplier to provide a schedule of proposed outcomes and milestones that would to be incorporated into the ADS overall scheduling and prioritisation.

**Purpose**

The purpose of this document is to define the Technical Cloud Architecture, Design, Security and Support (TCADSS) services required by ADS:

This document is split into three schedules:

**Introduction –** Summary of typical scenarios
**Background** – Background detail of ADS for understanding by all.
**Schedule 1** - The services required.
**Schedule 2** - The technology utilised.
**Schedule 3** -The service levels required.

**Background**

ADS provides hosting and through life application-based information services to the Army and wider Defence; predominantly through web applications accessible either from the intranet or from Defence infrastructure.

ADS as an organisation is made up of a core of Crown Servant personnel (Military and Civil Servants) and a series of contracted-out Technical Services. The Crown Servant population includes elements from 605 Signal Troop (10 Signal Regiment) that directly support ADS. The size of ADS fluctuates depending on the demand for the delivery of new products.

ADS is divided into two closely coupled Cloud Hosting and Software House arms:

**Army Cloud**. ADS provides Army Cloud application hosting capability across three security domains in the form of Official, Official-Sensitive and Secret. The official domain the Army Cloud capability is provided using MODCloud delivered Public/Community cloud deployments[1]. In the Official-Sensitive and Secret domains Army Cloud capability is provided in the form of a private cloud; known as the Army Hosting Environment (AHE). In addition to these hosting capabilities, some aspects of the software Development and Continuous Integration / Continuous Delivery (CI/CD) pipeline for delivery onto Army Cloud are in a commercial Microsoft Azure tenancy, enabling remote access to the agile development teams.

**Army Software House**. ADS builds bespoke software for the Army and wider defence to fill its niche functional requirements. It also develops Commercial Off The Shelf (COTS) based application solutions and data warehouse and analytics solutions as required.

ADS seeks to continue to expand and improve its application hosting solutions within its public / hybrid / private cloud and extend into the operational space as the Land specialist for systems and services. Using private cloud costing when security considerations dictate and Public/Community cloud hosting when the flexibility and cost is beneficial.

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

To leverage the current investment in infrastructure design & support, ADS looks to re-use as many common design and assurance principles as possible within the Army Cloud to provide a commonality across all cloud deployments.

The TCADSS Services will be expected to work seamlessly with the incumbent and outgoing TCADSS team to maintain ADS's required outputs.

**Army Cloud - Army Hosting Environment (AHE), private cloud hosting**

The AHE is the 'private cloud' component of the Army Cloud. It is located on MOD premises, across two sites. It currently supports 145+ business applications across multiple security classifications. In the Official-Sensitive and Secret environments, this is connected to the military WANs and the applications are accessed from a MODNet web browser. ADS provides the hosting environments using fully Software Defined Data Centre technologies (SDDC).

The applications hosted on AHE support a wide range of functions across HR, logistics, intelligence, finance, command and control. These include the Enterprise Resource Management (Churchill), Operational Deployment Record (ODR) (training competency service) and System for Liability Information Management (SLIM) (organisational service). There are currently 145+ live application services on the Official-Sensitive, of which 50+ are Oracle APEX, 10+ are Microsoft .Net and the remainder are Commercial Off the Shelf (COTS) application suites. 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 and ESRI to provide mapping. 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 Analytics Server (OAS) and the Army Data Analytics Platform using Statistical Analysis Software (SAS), to provide reporting and analytics across the Army. On Secret, there are fewer application services, but this is anticipated to grow due to the lack of Secret hosting facilities across Defence. 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)).

ADS has moved 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.

ADS will expand the Army Cloud to use increasing components of Cloud Service Provider (CSP) public and community cloud solutions over the short to medium term. This will expand the Army 'hybrid' Cloud allowing centralised management and interoperability between apps and services that bridge security domains.

**Army Cloud - MODCloud 'public/community' cloud hosting**

The MOD's Defence Digital organisation provides public and community cloud hosting via assured services contracted from three of the main Cloud Service Providers (CSPs) – Amazon, Microsoft, Google and Oracle. ADS uses MODCloud hosting to expand its Army Cloud capability out into public and community cloud hosting. Application users access the MODCloud based applications from all standard internet-based devices (personal laptops, tablets, phones, etc.) but can also access them from the military WAN via the MOD Boundary Protection Service (BPS). ADS uses MODCloud, for example, to host the Defence Gateway (DGW) that supports 270,000 registered users across regulars, reserves, families, veterans and contractors. The DGW provides a Single Sign On (SSO) and Two Factor Authentication (2FA). Other capabilities provided include the Defence Learning Environment (DLE) and Westminster (Cadet information system) and approximately 80 other services of which about 25% are ADS delivered (the rest belonging to defence partners). These services are predominantly web applications with a handful of native mobile applications. The web services provided range including COTS, in the form of web e-mail, SharePoint (used as a Content Management System) and Jive (known as Defence Connect) and bespoke developed services that include, a portal page (consolidating access to all the services), Reserve Attendance & Pay Service (RAPS) and My Admin (provides pay statements).

**Operating Model**

ADS has invested significant time and effort to adopt Agile methodology and to mature as a DevSecOps organisation. A pipeline approach has been established for deploying onto the Army Cloud, maintaining common technologies where possible.

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.

The Service Operations and Management teams utilise ITIL for change, incident, problem, knowledge and asset management. BMC 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.

**ADS Organisation, roles and responsibilities**

A breakdown structure of ADS highlighting the key relevant teams is detailed in the paragraphs below.

The teams are either Crown Servant staffed or 'contracted out' services. Each set of contracted out services has an allocated Crown Servant 'Service Owner' who is responsible for prioritisation of the business outcomes and the escalation point of contact for communications between the services supplier and the wider ADS.

**Army CTO Pillar**. ADS is part of the Army Chief Technical Officer 'pillar'.

**Army Digital Services (ADS).** ADS is led by two Assistant Head (AH) grade Crown Servants (a Colonel and a B2 civil servant).

**Senior Leadership Team (SLT).** SO1 level business management team.

**Application Delivery**. This branch of the organisation fulfils the ITIL Service Delivery function.

- **Development Services – contracted out 'as a service'.** This service provides a scalable capability based, predominantly, on 6-person teams, comprising of 2 developers, 2 testers, Business Analyst (BA) and Scrum Master/Delivery Manager as their primary skills but all are multi-disciplined. These teams use SCRUM as their main framework for delivering software. There are normally in the region of 10 product teams at any one time working in ADS. This service also provides an In Service Development team that supports the fleet of applications that are not under active development.

**Web Services Team.** This team manages the business services that ADS provides to users needing internet facing access.

**Web Development Services – contracted out 'as a service'.** This provides a development service for the Web Management Team. It develops and supports new services that are deployed to internet facing hosting.

**Service Operations**. This branch of the organisation fulfils the ITIL Service Operations function.

**Technical Cloud Architecture Design and Security Support (TCADSS**) This provides the Technical Cloud Architecture Design Office and Security Support, and all the main technical services required by ADS, with subject matter experts (SMEs) for all the technologies employed in the Army Cloud. They are responsible for providing services to design, deploy, manage, and support infrastructure and platform services and providing 3rd and 4th line support for these services. The subject of this document and requirement**.**

**Application Support Team (AST).** The main role of the team is 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 Azure DevOps.

- **Application Support Services – contracted out ‘as a service’.** The provision of the technical services required to support Oracle and Microsoft databases used by Army Cloud.

**Operational Support Team (OST).** A team of civil servant and military personnel that monitors and provides 1st line support to the Army Cloud. For all technical matters they are supported and guided by service provided by the **TCADSS**.

**Security Operations Centre Team (SOC).** A team of civil servants and military that provide the front-line protective monitoring capability for ADS and the Army Cloud. Monitoring event feeds and generate alerts for unexpected events / logons etc.

**Technical Assurance Services (TAS) – contracted out ‘as a service’.** The TAS Team ensure ADS strategies, processes and policies are applied throughout project delivery. IT provides Services that are used to assure the outputs of the other contracted out services. This assurance covers Test, Development and Program Planning.

**Service Management.** A team of civil servants and military that provide the first line of support for Army Cloud applications.

**Data Team.** This team manages the use of data within Army Cloud. The Data Warehouse, Application Programming Interface (API) and Robotic Process Automation (RPA) capabilities.

- **Data Warehouse Services (DWS) – contracted out ‘as a service’.** 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 thus ensuring the use authoritative data.
- **Integration Services – contracted out ‘as a service’.** The provision off API capabilities across the Army Cloud.
- **RPA Services – contracted out ‘as a service’.** The provision off RPA capabilities across the Army Cloud.

**Schedule 1 – Services**

The TCADSS service is to design, deliver, and support activities in relation to Army Cloud and its platforms and services to include extending into the deployed/operation space. This will entail utilising existing cloud environments, and any new capabilities delivered by the TCADSS capability.

The service will provide a Through-Life Design Authority and Specialist Engineering Function for the It will ensure that ADS's platforms, systems, and services are designed, assured, and operated in line with enterprise architectural principles, security requirements, and technology strategy.

The service will:

- Act as the design authority for solutions, systems, and services.
- Provide solution, security, and platform architecture capability.
- Deliver 4th line engineering support for complex technical escalations.
- Ensure designs remain aligned to business outcomes, compliance, and future scalability.
- Support projects by reviewing and approving solution designs.
- Review and govern service changes with significant design or security impact.
- Provide final-level escalation for complex incidents and outages.
- Define and evolve architectures for cloud migration and new service introduction.
- Support Client audits, accreditation, and compliance obligations.

All requirements will come in via the organisations ITSM, prioritised by the business for the contracted service to then deliver. The types of work that comes in will fall into the service categories below.

Individuals that fulfil this requirement MUST hold Security Check (SC) as a minimum.

If contractors delivering these service require regular access to the server rooms, for scenarios such as hardware upgrades and configuration then they MUST hold Developed Vetting (DV).

The following key, high level, service types are required:

| **Service Id.** | **Service Name** | **Description** |
|---|---|---|
| TCADSS -1 | Design authority | Provide expert advice on the tools, technology and methodologies use for Army Cloud solutions and act as the ADS Design Authority, providing expert technical advice and guidance to, and on behalf of, ADS. |
| TCADSS -2 | Secure Design and Compliance | Deliver secure Army Cloud solutions following the appropriate security principles. Deliver the Solution Architecture and Compliance services required to support the accreditation of the Army Cloud to legal, MOD and industry regulations and standards. |
| TCADSS -3 | Service Scoping | Create models and standards for scoping and costing Army Cloud solutions (including mechanisms for the production of estimates and invoices). |
| TCADSS -4 | Management and planning | Provide the technical planning, management and communications required to deliver the TTCADSS services that ADS requires. |
| TCADSS -5 | Platform Engineering | Support the Army Software house to ensure that designs are optimal and by delivering Platform Engineering automation services utilising industry leading technologies. To Support a DevSecOps delivery approach. |
| TCADSS -6 | Design Review | Produce and review technical design documentation produced by ADS and wider defence. |
| TCADSS -7 | Technical Support | Provide ad hoc support to troubleshoot Army Cloud incidents (3rd/4th line support). |
| TCADSS -8 | Policies and Standards | Develop policies and standards for the Army Cloud and ADS and provide technical assurance against these policy and standards. |

|  |  |  |
|---|---|---|
| TCADSS -9 | Platform Delivery | Deliver design, build, patch, upgrade and support for Army Cloud platform operating systems and platform/system software. |
| TCADSS -10 | Infrastructure Delivery | Deliver design, build, patch, upgrade and support for Army Cloud Infrastructure hardware and software. |
| TCADSS -11 | Network Delivery | Deliver design, build, patch, upgrade and support for Army Cloud Network hardware and software. |
| TCADSS -12 | Technology Selection | Evaluate products and proposed solutions against ADS business objectives. Undertake proof of concepts. Help ADS to select value for money solutions. |
| TCADSS -13 | Systems Integration | Design and implement secure integration between MOD systems and the Army Cloud. |
| TCADSS -14 | Cloud Migration | Implement cloud environments and migrate workloads between cloud environments. |
| TCADSS -15 | Tuning and Optimisation | Evaluation of Army Cloud performance and optimisation of systems components and designs where required. |
| TCADSS -16 | Technical Horizon Scanning | Ensure that any emerging or sunsetting technologies that may have benefit to or an impact on the Army cloud and ADS business are identified and evaluated. Piloting possible solutions. Recommending solution adoption where appropriate. |
| TCADSS-17 | Audit | Provide audit services should ADS require audits of other ADS team's service delivery. |
| TCADSS-18 | Security Monitoring and Observability | Delivery of core security platforms that cover the depth and breadth required to include EDR, SIEM, SOR, Vulnerability Scanning and health monitoring. |
| TCADSS-19 | Core Enabling Services | Domain administration and core services like anti-malware and patching. |
| TCADSS-20 | PaaS Scalability | Provide the subset of the above services required to provide ADS customers with a Platform as a Service (PaaS) delivery that does not impact the ADS priorities. |

**Below is a key list of service functions that will be required:**

**Architectural Authority**

- Establish and maintain solution and security architecture patterns.
- Govern solution designs, ensuring alignment to the client's enterprise principles.
- Conduct design reviews, risk assessments, and technical impact analysis.
- Approve or reject solution designs submitted by projects, Tenants or 3rd parties.

**Hybrid Multi-Cloud Architecture**

- Define, evolve, and assure ADS's hybrid cloud reference architecture (across Azure, AWS, GCP, and on-prem).
- Specify integration patterns, networking, identity, and workload portability.
- Develop cloud landing zones and guardrails to support compliance and operational efficiency.

**Security Architecture & Assurance**

- Define security reference models and controls across multi-cloud and legacy platforms.
- Conduct threat modelling and risk analysis of solutions and services.
- Define security patterns for zero-trust, data protection, identity management, and monitoring.
- Support accreditation and assurance activities.

**Through-Life Engineering Authority**

- Provide 4th line expertise for escalated incidents that cannot be resolved by operations.
- Analyse root causes of complex failures and define remediation strategies.

- Approve changes with major design or security impact.
- Ensure platforms evolve in line with design intent, reducing technical debt.

### Continuous Improvement & Road mapping

- Define technology roadmaps to align with client strategy.
- Identify opportunities for optimisation and automation.
- Recommend decommissioning, consolidation, or refactoring activities.

**Key Scenarios to be delivered by the Service:**

- **Project Design Support:** Assuring new solution designs before implementation.
- **Service Change Approval:** Reviewing major service changes to ensure compliance with design authority.
- **Cloud Adoption & Migration:** Designing and assuring migration of workloads to hybrid cloud platforms.
- **Incident Escalation:** Acting as the final technical escalation layer for critical incidents.
- **Security Assurance:** Providing designs, risk mitigations, and support for audits and accreditations.
- **Continuous Evolution:** Updating architectures in response to emerging technologies and threats.

The business outcomes required by ADS each month will be prioritised and agreed in advance with the supplier by the Service Owner. The supplier will provide the appropriate service to deliver these outcomes. Confirmation of the delivery / partial delivery of outcomes will take place at month end.

The service must deliver:

- Solution, Security, and System Architectures aligned to Enterprise Architecture.
- Reference environments and landing zones delivered for development and operations.
- Platform engineering artefacts (infrastructure-as-code, build scripts, automation templates).
- Performance and resilience assurance reports validating designs against NFRs.
- Security assurance evidence embedded into platforms and development pipelines.
- Infrastructure and platform project outcomes, including design, build, and handover.
- Root cause analysis and remediation reports for critical incidents.
- Technical roadmaps showing evolution of platforms to support development needs.
- Security architectures and models that embed regulatory and organisational security requirements.
- System architectures and designs that ensure interoperability, resilience, and lifecycle integrity.
- Design compliance reports showing alignment of solutions to Enterprise Architecture standards.
- Reference architectures, roadmaps, and reusable design patterns for hybrid multi-cloud adoption.
- Infrastructure project outcomes including designs, builds, and handovers.
- Healthchecks, technical assessments, and compliance reviews for systems and services.
- Advisory reports and strategic guidance provided directly to the CTO and executive forums.

The Design Office (with Platform Engineering) will be engaged to:

- Design and assure environments for new projects and services.
- Support development teams with platform integration and deployment.
- Provide security and resilience assurance during system design and testing.
- Provide 4th line escalation for environment-related issues affecting development or production.
- Support technology refresh and lifecycle upgrades across environments.
- Support programmes and projects by producing and assuring Solution, Security, and System Architectures.
- Conduct security and architectural healthchecks of existing platforms and services.
- Govern significant service changes with security or architectural impact.
- Provide impact assessments for deviations from Enterprise Architecture standards.
- Deliver infrastructure projects, managing requirements, risks, and technical transition.
- Act as a technical advisor to the CTO, providing insights into disruptive technologies and long-term risks.

The supplier will be required to work with other suppliers/strategic partner~~'s resource~~s and internal staff to ensure a coherent delivery of service (including any incumbent team during contract handover).

**Schedule 2 –Technology**

This schedule details the key technologies that currently underpin the services detailed above. The service provider must be experienced in the design, configuration, delivery, and maintenance of all aspects of these technologies (excepting those marked 'peripheral') and to be able to provide 3rd and 4th line support.

Server Infrastructure

| Compute | Relevance |
|---|---|
| The AHE currently uses Cisco UCS servers, blades and chassis to provide its compute capability for its private cloud. | The majority of server infrastructure is virtualised with limited exceptions.<br>The Army Hosting Environment consists of two components: one with approximately 2600 VMs and another with 400 VMs. |

Network Management

| Networking | Relevance |
|---|---|
| As well as the NSX-T software defined networking the AHE currently uses Cisco Nexus with ACI, Fortinet NGFW for North-South traffic, QoS and IPS.<br>The Network is split across the Primary and DR sites and a dedicated 10G DWDM site to site link utilising ADVA hardware provided by BT.<br>Enterprise Catapans are utilised to provide secure links between the sites.<br>VMWare Aria Automation is utilised for self-service provision.<br>Cisco Meraki MX Appliances, MR Access Points and Cloud managed Switches for internet facing systems and services. | The base position used is a zero-trust configuration (i.e. total platform isolation). |

Storage Area Networks.

| Storage | Relevance |
|---|---|
| The AHE currently uses Pure storage arrays: (https://www.purestorage.com/uk/). | The majority of storage is SAN based (limited use of DAS). This storage is usually presented to the hypervisor which is then formatted as VMFS.<br>The Systems are configured as Dark site and configured to use Pure1 Unplugged.<br>Supplied resource are required to be Pure dark site certified for both Flash Array and Flash Blade in order to be authorised to manage and upgrade these devices. |

VMware Virtualisation and Management Technologies.

| Broadcom (VMware) Products | Relevance |
|---|---|
| to include;<br>ESXi<br>vCenter<br>ARIA Automation<br>ARIA Operations<br>NSX-T<br>Site Recovery Manager | The AHE component of the Army Cloud solution (Army Cloud – Private) is a Software Defined Data Centre (SDDC) based on VMware technology and some these are additionally used to support the expanded Army Cloud (e.g. health monitoring the public cloud elements). |

Operating systems.

| Operating Systems | Relevance |
|---|---|
| RedHat Linux 7.x /8.x/9.x<br>Microsoft Server 2016/2019/2022/2025 | All Army Cloud platforms are built using scripted installs onto hardened versions of these operating systems that are the responsibility of the team to deliver and maintain. |

Oracle System software.

| Oracle Software | Relevance |
|---|---|
| Oracle RDBMS (including RAC, RMAN and ASM)<br>Oracle Weblogic. (including SAML2)<br>Oracle Access Manager (including Kerberos)<br>Oracle Virtual Directory<br>Oracle Internet Directory<br>Oracle Analytics Server (formally Oracle Business Intelligence EE)<br>Oracle BI Publisher<br>Oracle APEX and ORDS<br>Oracle Fusion middleware<br>Oracle Data Vault, VPD and TDE<br>Oracle Data Integrator<br>Oracle Enterprise Manager<br>Shibboleth (open source)<br>Oracle Cloud Infrastructure (OCI) | Key elements of the ADS Oracle platform reference architecture. |

Microsoft System software.

| Microsoft Software | Relevance |
|---|---|
| AD<br>ADFS<br>SharePoint<br>SQL Server<br>Reporting Services<br>CRM Dynamics 365<br>Azure DevOps<br>Azure<br>Release Manager<br>IIS<br>SCCM | Key elements of the ADS Microsoft Application Platform reference architecture. |

Redhat System Software.

| Redhat Software | Relevance |
|---|---|
| Redhat Resilient Storage<br>Ansible Automation<br>Redhat Satellite<br>PGP<br>Redhat Enterprise Linux<br>US DoD, STIG and NATO Common Criteria security best practice. | Key elements of the ADS Linux Platforms. |

The following SAS products are used:

| SAS | Relevance |
|---|---|
| SAS 9.4/Viya3.5/Viya 4.0 | PaaS is provided to the Analytics team as a Managed RHEL O-S with CFS. |

The following methods are used for identification and authentication.

| Identification, authentication Management | | Relevance |
|---|---|---|
| **AHE standard authentication** | The MOD WAN-based authentication is currently based on Microsoft Active Directory (AD) linked from the MOD desktop infrastructure to the AHE using 2-way cross forest trust. | The SSO between the user workstations and web based applications supported by the Oracle Platforms is based on Shibboleth supported SMAL2 (with a possible future move to OpenId Connect). |
| **MODcloud standard authentication** | The DGW in MODCloud is a open standards authentication and SSO system. This is based on Microsoft AD FS. | The SSO between the user and internet facing web based applications is provided by the DGW. The applications connect to the DGW using SAML2 or OpenId Connect. |

All applications delivered by ADS are automated using Continuous Integration and Delivery.

| Automated application delivery | | Relevance |
|---|---|---|
| **Performance Testing** | opentext LoadRunner. | Performance test tool. |
| **AV and Anti-Malware** | ADS primarily use Trellis / ePO, MOVE and MS defender. | Army Cloud anti-malware solutions. |
| **Integration and Release** | The integration and delivery of application code artefacts is supported using Microsoft Azure DevOps. | These applications will interact with the Oracle and Microsoft platforms and integration troubleshooting will be required. |
| **Source control** | All software is loaded into GIT(ADO) or GITLAB. | All source (e.g. configuration scripts) must be loaded into GIT (ADO) or GITLAB. |
| **Containerisation and Orchestration** | VMware Tanzu (Foundry), Docker. | Technologies available to support containers. |
| **KMS** | Gemalto Key Management | Centralised Keys Manager for encryption at rest. |
| **Privileged access management (PAM)** | The Delinia (Thycotic Secret Server) application is used for the management of server account passwords. | All automation scripts need to integrate with the Secret Server REST interface. |
| **Confluence/JIRA** | Document meta data management and control | Used primarily as a centralised Information Management tool (ISMS) to support the Technical and Security Architecture and provide evidence to meet JSP 453 and Compliance/Accreditation requirements. |
| **Hardware Security Module (HSM)** | Thales –SafeNet Luna appliances | Used to store the private keys for the PKI solution. ADS is a Defence level 1 certificate Authority, and the supplier will be required to operate this service. |
| **Static code testing** | All application code is subject to static testing that covers:<br>Coding standards (using TOAD)<br>Vulnerability scanning e.g. SQL Injection and Cross Site scripting (using APEXSEC and CheckMarx). | **Peripheral relevance to this service**. These applications will interact with the Oracle and Microsoft application platforms and integration troubleshooting will be required. |
| **Automated functional testing** | ADS uses the following toolsets for automated functional testing of applications and APIs.<br>Mocha, Chai, Cypress, Javascript, Selenium/Java, F#/ Canopy | **Peripheral relevance to this service**. These applications will interact with all platforms and integration troubleshooting will be required. |

All platform configuration changes are undertaken using automation.

| Automated system software delivery | | Relevance |
|---|---|---|
| **Automated delivery** | ADS uses Red Hat Ansible, SSCM, ADO for the automated delivery of changes to the system software underpinning a Infrastructure and System Software components. Aria Automation is used for self-service provision of infrastructure. | The aim of the organisation is to make the live platforms as ‘human free’ as possible as far as change goes.  All changes to platform configuration, however small, has to be scripted and delivered via Ansible Tower. |

Protective Security Monitoring.

| Security Incident Event Management | | Relevance |
|---|---|---|
| **SIEM** | The AHE utilises ArcSight as the Security Incident and Event Management (SIEM) System | This needs design, development and support through life. Plus possible eventual replacement with a new solution. |
| **Logging** | All Army cloud infrastructure, platforms an applications should send logs to the SIEM system. | All Infrastructure and Platforms are configured to provide syslog or CEF formatted security logs to the ESM and Logger. |

Proactive Health Monitoring.

| Proactive Monitoring | | Relevance |
|---|---|---|
| **Monitoring** | Cisco Data Center Network Assurance and Insights suite<br>Cisco Intersight Cloud Operations Platform<br>Aria Operations provides centralised reporting and health monitoring of both physical and virtual infrastructure. Supports Show back/Charge back cost model.<br>Oracle Enterprise Manager | Key tools for system monitoring and support |

Large 3rd Party Capabilities.

| Large 3rd Party Capabilities | | Relevance |
|---|---|---|
| | ESRI ArcGIS Server Suite<br>SAS – Statistical Analysis Software, Viya and Visual Analytics Suites<br>Software AG Suite of technologies to include API Gateway, API Portal, Integration Server, Web Methods, Alfabet. | Large 3rd Party vendor products and are deployed and configured as Platforms within the AHE Private Cloud. |

**Schedule 3 – Service Levels**

The supplier is expected to provide the Services with the outputs detailed within the Service Order Form.

The supplier should provide resources with a level of technical competence based on validated work history and proven expertise operating at the levels and in a similar role and discipline, with any complementing or required qualifications, these should include, but are not limited to, the following:

**Mandatory assurance levels**

Security Experience:

The Lead Security role must have demonstrated experience of at least 7 years working as a senior risk advisor to Government/Defence or FTSE equivalent organisations.

**Architecture and Design**

Technology Qualifications

Pure Storage 'lights out' certification (required by Pure for the supplier to be able to apply patches to the AHE SAN due to the 'dark site' status of the systems).

L3 Harris – Catapan certified and Crypto authorised personnel

Desirable assurance levels:

Cloud Service Provider certification (e.g. AWS, Azure and OCI).
Other security and technology qualifications.

The supplier and the resources provided must be free of any commercial ties or obligations to any hardware or software vendors.

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

**Scaling.** This shall be detailed in the Service Order Form, and the priority shall be agreed by the Authority and Supplier.

**Out of Hours Support.** This shall be detailed in the Service Order Form, and shall be agreed by the Authority and Supplier.

The majority of work can be planned and scheduled within core business hours however out of hours support may be required in order to perform a large platform, infra, or application upgrade that would otherwise cause a significant disruption to service. ADS would further require a mechanism to gain access to the relevant domain experts in the event a Severity 1 escalation occurs to would likely take to forms;

Security Incident – Once the SOC have carried out their initial investigation, technical advice may be required on suitable COA's.

Or

Critical System(s) or Service(s) become unavailable – The Applications and services support planning and under certain circumstances provide support to Operations in these instances dependent on the nature and severity of the issue the Authority requires the option to request out of hours support.

**Government Furnished X (GFX).** The supplier will be expected to provide equipment capable of supporting the internet facing elements of the TCADSS service delivery. Due to the security requirements of the higher classification elements of the Army Cloud, adequate GFX will be supplied by ADS to support TCADSS service delivery to these elements.

GFX Deliverables required from the Authority shall be detailed within the Service Order Form.

**Use of Authority Information Systems and Repositories.** The **Supplier** shall, for the purposes of fulfilling its obligations under this Agreement, access and utilise the Client's designated Information

Technology Service Management (ITSM) system, Information Security Management System (ISMS), and associated information repositories. These shall include, without limitation:

- **Confluence** for documentation and knowledge management.
- **SharePoint** for document storage, collaboration, and controlled information sharing; and
- **GIT repositories** for the storage, version control, and management of source code e.g. Infrastructure as Code (IaC).

The Supplier shall ensure that all Deliverables, documentation, source code and related materials produced in connection with the Services are created, maintained, and stored within such systems as defined by the Client. The Supplier shall not utilise any external repositories, tools, or storage solutions for Client information or assets, save where expressly authorised in writing by the Client.

The Supplier shall be responsible for ensuring that its personnel engaged in the performance of the Services are suitably trained and competent in the use of the above systems and shall ensure compliance with all applicable Client policies, standards, and procedures relating thereto.

Nothing in this clause shall be construed as creating a relationship of employment, partnership, or joint venture between the Client and any personnel of the Supplier. The Supplier shall at all times retain responsibility for the supervision, direction, and control of its personnel, and shall provide the Services as an independent entity operating outside the scope of IR35.

**Licencing and Support Agreements.** ADS will ensure that all system software utilised by the Service Supplier is fully licenced with the provider of the software and that support agreements are in place to allow Service Requests to be raised by the service supplier against the software. this will include but not limited to:

Microsoft EA to include MSDN and Azure subscriptions.
Broadcom (VMware) EA.
Oracle EA to include Premier licence support.
Oracle Advanced Customer Services.
Red Hat standard support.
Cisco EA.
Pure support.
Fortinet Support
L3 Harris

**Hardware and Software Infrastructure Procurement.** ADS will be responsible for procurement of all the IT assets and equipment required to support the Army Cloud. The Technical Design Office Team will be responsible for defining the technical requirements to ensure the correct cloud capabilities can be procured to meet the requirements of the business.

**Intellectual Property Rights (IPR).** The selected supplier shall not retain IPR relating to any services, designs, documentation or configuration delivered during the term of the contract.

**Exit Plan.** 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.

**Contract Management.** The supplier is to attend frequent meetings with the authority. The supplier will be expected to provide a SoW which defines the recurring monthly activities, deliverables, and outcomes of the Design Office and Platform Engineering and Cloud support Services, covering Solution, Security, and System Architecture, Platform Engineering, Infrastructure Delivery, and support for Deployable Systems as they evolve. It is understood that the Supplier will deliver these functions on an ongoing, outcome-based basis. The specific scope and prioritisation will be defined by the Client's business and operational priorities each month, but the functions listed within the Core SoW remain in scope throughout the engagement.

**Service Flexibility.** The Supplier will allocate and manage its own resources to deliver the required outcomes. The specific mix of activities each month will vary according to ADS priorities, but the Supplier remains accountable for ensuring all functions are delivered to the required level of quality and completeness.

**Reporting.** The Supplier will provide a monthly service report covering:

- Key outcomes delivered (architecture artefacts, assessments, designs, reports).
- Governance activities supported.
- Risks, issues, and recommendations.
- Updates to roadmaps and reference architectures.

These details and format shall be included within the Service Order Form.

**Client Interface & Governance.** The CTO Pillar has established a B1 Chief Engineer/Architect, who is the ultimate owner of enterprise technical strategy.

The provided service is to interfaces with this client role or delegates, providing:

- **Design proposals** for approval.
- **Impact assessments** for major technology changes.
- **Incident reports** and remediation recommendations.
- **Architecture artefacts** and reference models.

Governance will be delivered by establishing **Architecture Review Boards (ARBs)**, **Design Authority Boards (DABs)**, and **Operational Escalation forums** where the service presents, advises, and assures solutions, but final accountability will remain with the client’s Chief Engineer/Architecture Group.

**Invoicing and Payment.** ADS expects the service supplier to invoice monthly against deliverables, part of fully delivered. No Later than the end of the first week of each month. (excluding Bank Holidays)

**Duration**. The duration of the overall need is assessed as 18 months from award.