715660450

The Provision of Army Digital Services (ADS) Security Test as a Service (STaaS)

(DInfoCom/0292)

Statement of Requirement

CONTENTS

1. PURPOSE

1.1 The MOD may be referred to as “the Authority” hereafter.

1.2 Army Digital Services (ADS) requires specialist technical support to provide CHECK Certified Code Assisted Security Assessments, IT Health Checks, Product Vulnerability Security Assessments & Penetration Testing on Non-LIVE Applications on both new and in-service Applications and Infrastructure. From time-to-time ADS will also require security assessments and reports on new technologies, e.g. the use of Data Diodes and security validation of the proposed solutions.

2. DURATION

2.1 The duration of the overall requirement is for a twenty-four (24) month period, from 15 Dec 2025 until 14 Dec 2027, with an option (currently unfunded) to extend the contract for a further twelve (12) month period.

3. LOCATION

3.1 The normal place of work for this requirement is Andover, Hampshire, U.K. Although a proportion of this work will be suitable for remote working, there will be routine occasions when team collaboration is essential, as is engagement with the user community, service delivery agencies and assurance entities. As such it is not considered to be appropriate that this requirement is satisfied by off-shore resources working outside the UK.

4. DEFINITIONS

Expression or Acronym	Description
ACP	Army Cloud Private
ADS	Army Digital Services
AHE	Army Hosting Environment
API	Application Programme Interface
AST	Application Support Team
BA	Business Analyst
BI	Business Information
BOS	Base Operating System
CD	Continuous Deployment
CI	Continuous Integration
COTS	Commercial off the Shelf
CPUs	Critical Patch Updates
CRM	Customer Relationship Management
CS	Civil Servant
DAIS	Defence Assurance and Information Services
DD	Defence Digital
DE&S	Defence Equipment & Support
DGW	Defence Gateway
DII	Defence Information Infrastructure
DOS	Digital Outcomes and Services
EGS	Enterprise Gateway Service
IDAM	Identity Access Management
ITHC	Information Technology Health Check

KPI	Key Performance Indicators
MI	Management Information
PaaS	Platform as a Service
PT	Penetration Testing
RACI	Responsible, Accountable, Consult and Inform
RAPS	Reserve Attendance & Pay Service
SAS	Statistical Analysis Software
SDDC	Software Defined Data Centre
Sig Sqn	Signal Squadron
SIT	System Integration Test
SSO	Single Sign On
TDO	Technical Design Office
VA	Vulnerability Assessment

5. BACKGROUND TO ARMY DIGITAL SERVICES (ADS)

5.1 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.

5.2 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 . 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.

5.3 **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).

5.3.1 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.

Operating Model

5.4 ADS has invested significant time and effort to adopt Agile and then start to mature as a DevOps organisation. A pipeline approach has been established for deploying onto both the ACP and ADS Managed MoDCloud, utilising the same technologies for the majority.

5.5 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. Significant investment has been made to automate testing.

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 DevOps ways of working.

5.6 **ADS Organisation, roles and responsibilities**

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. ADS is comprised of the following pillars of capability:

Applications Development:

Oracle

.Net

Power Apps

Deployed Apps

Infrastructure:

Technical Design Office

Application Support Team

Operation Support Team

Defence Gateway

Data:

Army Data Warehouse (ADW)

Integration as a Service (APIs)

Robotic Process Automation (RPA)

Security:

Compliance

Audit

Security By Design

Security Operations Centre (SOC)

Service Management:

Service Managers

Service Desk

Configuration Management

5.6 **Compliance Team.** Ensure ADS adheres to security and policies as laid out in Joint Service Publication (JSP) 440, 441 and 453 which replaced 604. The Compliance team ensures the delivery of new infrastructure and applications are secure and are Security Assured under Secure By Design (SbD), compliance with Network Joining Rules and Personal Information Asset Policy, maintenance of security and accreditation of existing services and auditing.

The Compliance team will manage the Cyber Security Testing as a Service Contract.

5.7 **Current Situation.** ADS utilises MoD internal teams in the form of Land Information Assurance (IA) Group (LIAG) and Joint Information Assurance Co-ordination Cell (JIAC) to conduct Vulnerability Testing of the Infrastructure. However, given the demand outstrips the ability of MoD capability to supply and the mandated requirement for cyber Security Testing, ADS has used the services of a third-party supplier to undertake ITHC's, VAs, PTs, product vulnerability research and Security Assessments.

6. TECHNOLOGY

6.1 The main technologies used by ADS to deliver the information services are detailed below the key technologies that currently underpin the services detailed above.

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. 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. 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. Enterprise Catapans are utilised to provide secure links between the sites. VMWare Aria Automation is utilised for self-service provision. 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. The Systems are configured as Dark site and configured to use Pure1 Unplugged. 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; ESXi vCenter ARIA Automation ARIA Operations NSX-T 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 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) Oracle Weblogic. (including SAML2) Oracle Access Manager (including Kerberos) Oracle Virtual Directory Oracle Internet Directory Oracle Analytics Server (formally Oracle Business Intelligence EE) Oracle BI Publisher Oracle APEX and ORDS Oracle Fusion middleware Oracle Data Vault, VPD and TDE Oracle Data Integrator Oracle Enterprise Manager Shibboleth (open source) Oracle Cloud Infrastructure (OCI)	Key elements of the ADS Oracle platform reference architecture.

Microsoft System software.

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

Redhat System software.

Redhat Software	Relevance
Redhat Resilient Storage Ansible Automation Redhat Satellite PGP Redhat Enterprise Linux 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.

6.2 **Automated Test**.

Static code testing	All application code is subject to static testing that covers: Coding standards (using TOAD) 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. 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.

7. OBJECTIVE AND DELIVERABLES

7.1 The service supplier is expected to use their “reasonable endeavours” to provide resources to meet the priorities specified by ADS. The delivery could be delivered by pre-determined agreed packages such as “small, medium, large” or tailored bespoke individual taskings which are to be determined between ADS Compliance and Supplier Vendor on award of contract.

The deliverables for the service are detailed in Table 1 below.

Ser	Requirement Type
1	**CHECK Certified Testing –** work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a CHECK Certified Vulnerability/IT Health Check of targeted Applications/Infrastructure. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement and the details of the Application including what is in scope of the test, the classification of the Test & resulting report, highlight any dependencies on either the ADS internal teams, Product Owner or the Vendor. Outline any issues which might impact on testing, for example the need DV clearance or special handling restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued by the Vendor to ADS Compliance for approval by the Product Owner and should detail the Scope of works, agree a realistic amount of time for the engagement to enable a thorough test, number of Testers required and the Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.
2	**Vulnerability Security Assessments/ITHC** – work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a Vulnerability/IT Health Check of targeted Applications/Infrastructure. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement and the details of the Application including what is in scope of the test, the classification of the Test & resulting report, highlight any dependencies on either the ADS internal teams, Product Owner or the Vendor. Outline any issues which might impact on testing, for example the need DV clearance or special handling restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued by the Vendor to ADS Compliance for approval by the Product Owner and should detail the Scope of works, agree a realistic amount of time for the engagement to enable a thorough test, number of Testers required and the Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.
3	

	Penetration Test – work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a Vulnerability/IT Health Check of targeted Applications. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement and the details of the Application including what is in scope of the test, the classification of the Test & resulting report, highlight any dependencies on either the ADS internal teams, Product Owner or the Vendor. Outline any issues which might impact on testing, for example the need DV clearance or special handling restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued by the Vendor to ADS Compliance for approval by the Product Owner and should detail the Scope of works, agree a realistic amount of time for the engagement to enable a thorough test, number of Testers required and the Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.

Table 1 – Types of Engagement

7.2 There is a potential need for up to 50 of the requirements in Table 1 to be ordered over the twenty-four (24) month core period, but that is not definitive, and could be more or less.

Engagements will be created under the following terms:

7.2.1 Each engagement will be pre-agreed and scoped with the selected supplier, culminating in the creation of an engagement-tasking document defining pre-requisites, required serials and deliverables.

7.2.2 Given the increasing demand for ITHC, VA and PT, the service must be able to provide PT/VA/ITHC within 30 working days of receipt of requirement.

7.2.3 The deliverable will be a full engagement report detailing the testing completed, vulnerabilities identified with criticality level and recommended remedial work to mitigate weaknesses found in the elements in the scope of test vulnerability. The report is to be issued within 5 working days of the test completion date.

7.2.4 Virtual Machines will be set up prior to testing to enable Testers to perform the Vulnerability Assessment, ITHC, Penetration Test. Bidders must understand that any storage devices used on OFFICIAL SENSITIVE or above systems must either be securely deleted to HMG approved standards or the hardware will be retained on the customer site for destruction. Where on site assignment is required (the default engagement), Virtual Machines must be set up prior to testing to enable Testers to perform the Vulnerability Assessment, ITHC or Penetration Test (the connection of supplier equipment is not allowed). The tester must supply a suitable VM Image (e.g. OVF), containing all tools required, at least 5 working days before the engagement for upload.

7.2.5 ADS must be able to use the contract for Cyber Security testing for non-ADS delivered requirements. This often takes the form of COTS and 3rd party Applications that require a VA/ITHC prior to hosting on ADS infrastructure. The service must be scalable to meet the demands of these requirements and be able to use separate UINs for payment.

8. PROVISIONING

8.1 Given the increasing demand for VA and PT, the Supplier must be able to provide Penetration Test / Vulnerability Assessment/ITHC within 30 working days of receipt of accepted proposal.

9. PROGRESS MEETINGS

9.1 The contractor will report to SO2/SO3 Compliance on a routine basis to confirm task priorities, stakeholder engagement and progress against contract deliverables:

9.1.1 Monthly scheduling review meetings.

9.1.2 Ad-hoc project meetings.

9.1.3 Quarterly stakeholder review meetings.

10. SECURITY REQUIREMENTS

10.1 The delivery partner must hold either SC or DV Clearance:

10.2 Most Vulnerability Assessments require the Tester to hold UK GOV Security Clearance (SC), however there is also a requirement for some Assessments to be carried out by Testers holding a minimum of UK GOV Developed Vetting (DV) Security Clearance

11. EXPERIENCE

11.1 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. Previous applied experience in Vulnerability Assessments, CHECK Certified Assessments and Penetration Testing with the technologies used within ADS.

11.1.1 Resources supplied must be suitably qualified and experienced to meet UKSC standards & or hold Cyber Essentials Plus certification and have some resources which have either one of the following qualifications, (ideally CHECK):

(a) CHECK.

(b) CREST.

11.1.2 Current working knowledge of MoD systems and networks and previous experience providing services to MoD or security services would be a benefit.

12. CONTINUOUS IMPROVEMENT

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

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

13. INTELLECTUAL PROPERTY RIGHTS (IPR)

13.1 The selected supplier shall not retain IPR relating to any services, designs, documentation or configuration delivered during the term of the contract.

14. EXIT PLAN

14.1 The Authority and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier has transferred all outcome reporting assessments to the Authority before the end date of the contract.

14.2 If there are material changes to the Services and a contract amendment has been put in place which requires an addition to the above exit plan, a Statement of Work (SoW) may be agreed between the Authority and the Supplier to specifically cover the exit plan.

15. TRAVEL AND SUBSISTENCE

15.1 Travel and Subsistence (T&S) must be in line with the MOD expenses policy. (see Appendix 1 to Order Schedule 5) and agreed prior to approval.

APPENDIX 1 - APPROXIMATE NUMBER OF TESTS BY TYPE AND SIZE

Type of Test - Details of Requirement	Size	Year 1 (Approximate number of Tests)	Year 2 (Approximate number of Tests)	Year 3 (Approximate number of Tests)
CHECK Certified Testing – work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a CHECK Certified Vulnerability/IT Health Check of targeted Applications/Infrastructure. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement, scope of test, classification, special handling restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued detailing Scope of works, timeframe, number of Testers required and Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Security Clearance –** including National Insurance Number & Nationality for validation purposes. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.	Small	8	10	8
	Medium	4	8	4
	Large	6	6	6
Vulnerability Security Assessments/ITHC – work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a Vulnerability/IT Health Check of targeted Applications/Infrastructure. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement, scope of test, classification, special handling	Small	12	32	15

restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued detailing Scope of works, timeframe, number of Testers required and Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.	Medium	11	27	9
	Large	4	10	3
<u>Penetration Test</u> – work alongside ADS Compliance, internal MOD developers with access to application source code and Product Owners (Subject Matter Experts) to perform a Penetration Test of targeted Applications/Infrastructure. **Scoping Required -** Use an agreed (agreed between Vendor & ADS Compliance) Scoping document to capture the requirement, scope of test, classification, special handling restrictions for critical systems, On-site or Remote Testing. **Proposal of Work –** A Proposal of Work should be documented and issued detailing Scope of works, timeframe, number of Testers required and Price breakdown & Total. **Security Clearance –** Details of Testers Security Clearance should be passed to ADS Compliance including their, Full Name, Date of Birth, Nationality, & National Insurance numbers, at least 2 weeks prior to any Testing. **Visitor Passes –** To enable entry onto site (predominantly Andover) details additional to the above (**Security Clearance**) will require Car details such as type/model/colour & registration. **Output Required:** A full report detailing the issues identified, criticality level, & remediation recommendations required.	Small	3	3	2
	Medium	2	3	2
	Large	0	1	1
	Total	**50**	**100**	**50**

APPENDIX 2 - SERVICE LEVELS AND SERVICE CREDITS

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
Completion of work as per Agreed Monthly Statement of Work	Completion	100%	**100%**	N/A
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**		
Performance to Pay Process	In accordance with agreed performance to pay progress, Suppliers submit, or provide input, to the following: • Accurate and complete agreed Deliverables in a timely manner. • Accurate and complete Acceptance certificates in a timely manner. • Accurate and complete Statement of Works (SOW) in a timely manner. • Accurate and complete invoices in a timely manner.	• All of the inputs are submitted in accordance with the preformance to pay process timescales and contain accurate and complete information.	• Inputs are later than prescribed in the performance to pay process but within 5 working days of the prescribed dates. • Inputs are incomplete or inaccurate.	• Inputs are later than 5 working days in the prescibed performance to pay process. • Inputs contain significant errors.
Partnering Behaviours and Added Value	• Supplier promotes positive collaborative working relationships within and across the Service team by acting in a transparent manner. • Supplier shows commitment to Buyer goals through adding value over and above the provision of compensated skilled personnel/services.	• No behavioural problems identified. • Buyer reviews attended and positive contributions made. • Added Value recognised by the Authority above provision of compensated skilled resource/services.	• Some minor behavioural problems. • Supplier only attends some meetings or provides minor contributions. • Supplier adds some value above provision of compensated resource/service, but this is not regarded as significant.	• Significant behavioural problems. • Supplier contributions are rare or insignificant and shows little interest in working with other suppliers. • No added value contributions recognised by the Authority.
People (Resourcing)	• Successful recruitment and placement of key resources/provision of services to meet the planned deliverables and contractual obligations. • The supplier proactively manages their resource skills against expected Service Outcomes by identifying issues early and in a timely fashion, addressing any deficits.	• Targets met for all resources/provision of Service.	• Targets met for most (50%+) resources/Service through no fault of the Buyer.	• Target missed for most resources/Service requested through no fault of the Buyer.
People (Delivery)	• All Supplier resources delivering services for the contracts are performing to the expected standard for the skill-set supplied. • All services delivered by the Supplier are to the required standard expected by the Authority.	• No resources are swapped out due to deficiency in skill set and/or no change of services is required.	• Minor issue noted with quality of work/standard of service. • Few contributions made within team.	• Resource is swapped out from Service due to deficiency in skill set. • Persistent issues with quality of

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
		• No problems identified with quality of work. • Supplier is making positive team contributions • Supplier skills/services meet the standards expected.		work/service noted (may be minor ones which have persisted from one month to another). • Significant issues with quality of work/service noted in a month.

ADS_Balance_Scorecard.xlsx