**RM6100 Technology Services 3 Agreement**

**Framework Schedule 4 - Annex 1**

**Lots 2, 3 and 5 Order Form**

**Order Form**

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms.

The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website <http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm6100>. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”
2. Attachment 1 – Services Specification
3. Attachment 2 – Charges and Invoicing
4. Attachment 3 – Implementation Plan – NOT APPLICABLE
5. Attachment 4 – Service Levels and Service Credits – NOT APPLICABLE
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors
7. Attachment 6 – Software – NOT APPLICABLE
8. Attachment 7 – Financial Distress
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects – NOT APPLICABLE
11. Attachment 10 – Transparency Reports
12. Attachment 11 – Ad-Hoc Tasking Order Form
13. Attachment 12 – Monthly Statement of Work template
14. Attachment 13 – Statement Relating to Good Standing
15. Attachment 14 – Expenses Policy
16. Attachment 15 – Cyber Implementation Plan
17. Attachment 16 – Supplier’s Response; and
18. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

### the Framework, except Framework Schedule 18 (Tender);

### the Order Form;

### the Call Off Terms; and

### Framework Schedule 18 (Tender).

**Section A**

**General information**

|  |  |
| --- | --- |
| **Contract Details** | |
| **Contract Reference:** | 701576584 (DInfoCom/0175) |

|  |  |
| --- | --- |
| **Contract Title:** | Provision of Technical Design Office (TDO) |

|  |  |
| --- | --- |
| **Contract Description:** | The ADS TDO is responsible for:  a. The Planning, Design and Build of the Platforms and infrastructure underpinning the AHE (private cloud), JSF (public cloud) and MODcloud (Defence public cloud) to meet the anticipated requirements of Army and wider Defence.  b. Acting as the Design Authority of the Systems.  Work alongside the Support Service teams to maintain and support the Private cloud infrastructure and the public / hybrid cloud platforms on which ADS delivered applications and services run.  c. Ensuring that the AHE and JSF are secure and accreditable systems (with respect to MOD CyDR and the relevant JSPs).  d. Providing 3rd/4th line support for the in-service AHE and JSF infrastructure and platforms. |

|  |  |
| --- | --- |
| **Contract Anticipated Potential Value:** this should set out the total potential value of the Contract | £4,983,333 ex VAT (Core) Maximum  £4,900,000 ex VAT Non-Guaranteed Ad-Hoc Tasking Value for any additional work utilising Ad-Hoc Tasking Order Form upon receipt of approved Business Cases  In any instance Attachment 2 Part C Firm Priced Man-Day Rates will be utilised for both CORE & AD-HOC Activities |

|  |  |
| --- | --- |
| **Estimated Year 1 Charges:** | £2,440,096 ex VAT |

|  |  |
| --- | --- |
| **Commencement Date:** this should be the date of the last signature on Section E of this Order Form | 1 January 2022 |

|  |
| --- |
| **Buyer details** |
| **Buyer organisation name**  Army D Info Commercial |

|  |
| --- |
| **Billing address**  Your organisation’s billing address - please ensure you include a postcode  Blenheim Bldg, IDL 1, Army HQ, Andover, Hampshire, SP11 8HJ. |

|  |
| --- |
| **Buyer representative name**  The name of your point of contact for this Order  REDACTED MCIPS |

|  |
| --- |
| **Buyer representative contact details**  Email and telephone contact details for the Buyer’s representative. This must include an email for the purpose of Clause 50.6 of the Contract.  0300 164 8453; REDACTED@mod.gov.uk |

|  |
| --- |
| **Buyer Project Reference**  Please provide the customer project reference number.  Click here to enter text. |

|  |
| --- |
| **Supplier details** |
| **Supplier name**  The supplier organisation name, as it appears in the Framework Agreement  boxxe Limited |

|  |
| --- |
| **Supplier address**  Supplier’s registered address  Floor 2 & 3 Artemis House, Eboracum Way, York, YO31 7RE |

|  |
| --- |
| **Supplier representative name**  The name of the Supplier point of contact for this Order  REDACTED |

|  |
| --- |
| **Supplier representative contact details**  Email and telephone contact details of the supplier’s representative. This must include an email for the purpose of Clause 50.6 of the Contract.  [REDACTED@boxxe.com](mailto:REDACTED@boxxe.com); 01347 812100 |

|  |
| --- |
| **Order reference number or the Supplier’s Catalogue Service Offer Reference Number**  A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier’s Catalogue Service Offer Reference Number.  N/A |

|  |
| --- |
| **Guarantor details**  *Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.* |
| **Guarantor Company Name**  The guarantor organisation name  *Not Applicable* |

|  |
| --- |
| **Guarantor Company Number**  Guarantor’s registered company number  *Not Applicable* |

|  |
| --- |
| **Guarantor Registered Address**  Guarantor’s registered address  *Not Applicable* |

**Section B**

**Part A – Framework Lot**

|  |  |
| --- | --- |
| **Framework Lot under which this Order is being placed**  *Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.* | |
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | **X** |
| 1. TRANSITION & TRANSFORMATION | ☐ |
| 1. OPERATIONAL SERVICES |  |
| a: End User Services | ☐ |
| b: Operational Management | ☐ |
| c: Technical Management | **X** |
| d: Application and Data Management | ☐ |
| 1. SERVICE INTEGRATION AND MANAGEMENT | ☐ |

**Part B – The Services Requirement**

|  |
| --- |
| **Commencement Date**  See above in Section A |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Contract Period**  *Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:*   |  |  | | --- | --- | | **Lot** | **Maximum Term (including Initial Term and Extension Period) – Months (Years)** | | **2** | 36 (3) | | **3** | 60 (5) | | **5** | 60 (5) | | | |
| **Initial Term** Months  *24 Months (2 year)* | **Extension Period (Optional)** Months  *Not applicable* | |
| **Minimum Notice Period for exercise of Termination Without Cause**  (Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)* | | *30* |

|  |
| --- |
| **Sites for the provision of the Services**  *Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.*  The Supplier shall provide the Services from the following Sites**:**  **Buyer Premises:**  Army Digital Services (ADS), Ramillies Bldg, Army HQ, Andover, Hampshire, SP11 8HJ  **Supplier Premises:**  *Floor 2 & 3 Artemis House, Eboracum Way, York, YO31 7RE*  **Third Party Premises:**  *Not applicable* |

|  |
| --- |
| **Buyer Assets**  *Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms*  Microsoft EA to include MSDN and Azure subscriptions  WMware ELA  Oracle Premier licence support  Oracle Advanced Customer Services  Red Hat standard support  HPe Support  Cisco SmartNet Support  Pure Support  Corporate desktop and email system (MODNet laptops)  Corporate wifi  Access to buildings and data centres as required for the supplier to deliver the service  Provision of hot desk areas and on-site meeting room facilities |

|  |
| --- |
| **Additional Standards**  Guidance *Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*  *As detailed within the Statement of Requirement* |

|  |
| --- |
| **Buyer Security Policy**  *Guidance Note: where the Supplier is required to comply with the Buyer’s Security Policy then append to this Order Form below.*  *As detailed within the Statement of Requirement* |

|  |
| --- |
| **Buyer ICT Policy**  *Guidance Note: where the Supplier is required to comply with the Buyer’s ICT Policy then append to this Order Form below.*  *As detailed within the Statement of Requirement* |

|  |
| --- |
| **Insurance**  *Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.*  Third Party Public Liability Insurance - £1M default  Professional Indemnity Insurance - £1M default  Employer’s Liability Insurance - £5M minimum default |

|  |
| --- |
| **Buyer Responsibilities**  *Guidance Note: list any applicable Buyer Responsibilities below.*  *Not Applicable* |

|  |
| --- |
| **Goods**  *Guidance Note: list any Goods and their prices.*  *Not Applicable* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Governance – Option Part A or Part B**  *Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.*   |  |  | | --- | --- | | **Governance Schedule** | **Tick as applicable** | | Part A – Short Form Governance Schedule | X | | Part B – Long Form Governance Schedule | ☐ |   The Part selected above shall apply this Contract. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Change Control Procedure – Option Part A or Part B**  *Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.*   |  |  | | --- | --- | | **Change Control Schedule** | **Tick as applicable** | | Part A – Short Form Change Control Schedule | X | | Part B – Long Form Change Control Schedule | ☐ |   The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):   * for the purpose of Paragraph 1.3.2 (a), the figure shall be £NOT APPLICABLE; and * for the purpose of Paragraph 8.2.2, the figure shall be £NOT APPLICABLE. |

OT APP

**Section C**

**Part A - Additional and Alternative Buyer Terms**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Additional Schedules and Clauses** *(see Annex 3 of Framework Schedule 4)*  *This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.*  **Part A – Additional Schedules**  *Guidance Note: Tick any applicable boxes below*   |  |  | | --- | --- | | **Additional Schedules** | **Tick as applicable** | | S1: Implementation Plan | ☐ | | S2: Testing Procedures | ☐ | | S3: Security Requirements (either Part A or Part B) | Part A ☐ or Part B☐ | | S4: Staff Transfer | ☐ | | S5: Benchmarking | ☐ | | S6: Business Continuity and Disaster Recovery | ☐ | | S7: Continuous Improvement | **X** | | S8: Guarantee | ☐ | | S9: MOD Terms | **X** |   **Part B – Additional Clauses**  *Guidance Note: Tick any applicable boxes below*   |  |  | | --- | --- | | **Additional Clauses** | **Tick as applicable** | | C1: Relevant Convictions | **X** | | C2: Security Measures | **X** | | C3: Collaboration Agreement | ☐ |   Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.  **Part C - Alternative Clauses**  *Guidance Note: Tick any applicable boxes below*  The following Alternative Clauses will apply:   |  |  | | --- | --- | | **Alternative Clauses** | **Tick as applicable** | | Scots Law | ☐ | | Northern Ireland Law | ☐ | | Joint Controller Clauses | **X** |   Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract. |

**Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A**

|  |
| --- |
| **Additional Schedule S3 (Security Requirements)**  *Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of “Security Management Plan” insert the Supplier’s draft security management plan below.*  *Not Applicable* |

|  |
| --- |
| **Additional Schedule S4 (Staff Transfer)**  *Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of “Fund” in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.*  *Not Applicable* |

|  |
| --- |
| **Additional Clause C1 (Relevant Convictions)**  *Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of “Relevant Convictions” insert any relevant convictions which shall apply to this contract below.*  Any convictions other than minor road traffic offences |

|  |
| --- |
| **Additional Clause C3 (Collaboration Agreement)**  *Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.*  *Not Applicable*  An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Daysfrom the Commencement Date:  *Not Applicable* |

**Section D**

**Supplier Response**

|  |
| --- |
| **Commercially Sensitive information**  Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*  Supplier bid submission documentation, including Pricings and Workforce information |

**Section E**

**Contract Award**

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

|  |
| --- |
| **SIGNATURES** |

**For and on behalf of the Supplier**

|  |  |
| --- | --- |
| Name | **REDACTED** |
| Job role/title | **Contracts Manager** |
| Signature | **REDACTED** |
| Date | **16 December 2021** |

**For and on behalf of the Buyer**

|  |  |
| --- | --- |
| Name | **REDACTED** |
| Job role/title | **Army DInfo Comrcl SCO** |
| Signature | **REDACTED** |
| Date | **16 December 2021** |

**Attachment 1 – Services Specification**

# OUTCOME

1. Architect and maintain the Army Hosting Environment (AHE) (private cloud) and Joint Server Farm (JSF) (public cloud) across the hardware and software and specialist technical architecture domains (servers, storage, networks, database, Oracle, Microsoft, HPe, Pure Storage, Cisco switches and compute, and VMware) required to deliver a data centre to host applications and services in Defence. The service will also need to provide the necessary skills and expertise to maintain, support and change the technical architecture and design of Army Digital Services (ADS) digital ICT Cloud solutions including IaaS, PaaS and SaaS-based services (Infrastructure / Platform / Software as a Service) using the technology detailed in paras 32 to 46. The service will ensure the technical architecture is secure and compliant with Defence policies and industry best practice. In addition to maintaining a private cloud(s), there will be a need to architect the extension of the solution to be hybrid and have the capability of supporting cloud-native workloads. Those individuals that fulfil this requirement will need vetting to SC as a minimum. For those with regular access to the datacentre facilities or roles requiring privileged access to systems, DV will be required. In accordance with the framework conditions, the Authority will sponsor the relevant level of vetting. It is essential that the supplier holds enough personnel with the appropriate vetting status to conduct the handover[[1]](#footnote-1) from the current incumbent at the contract start date.
2. The outcomes required include:

* **Firewall management** – ensuring that the Army Private Cloud and Public Cloud maintain a secure perimeter. Ensure that the firewalls are deployed, patched and monitored to reduce risk to AHE and to manage any compliance risks.
* **Hosting** – manage the Army private cloud (on premise, traditional datacentre) and the JSF/MODcloud (cloud hosted infrastructure).
* **Incident management** – support the management of service affecting incidents on the public and private clouds.
* **Monitoring** – ensure that the relevant logging and alerts are passed to the Security Operations Centre (SOC).
* **Network administration** – regularly review and upgrade the hardware (compute, storage etc.). and any of the software systems (e.g. VMware software defined data centre) components to maintain a highly available system.
* **Systems administration** – install and support the physical and virtual infrastructure. Assist in 3rd and 4th line support of issues. Set appropriate security policies to control access to the environment following the “least privileged” access model.
* **Continuous Integration / Continuous Development** – support the CI/CD pipeline by deploying the relevant tools. This can include both on premise capabilities and tooling to take AWS / Azure artefacts into the relevant production environment.

# Purpose

1. The purpose of this document is to define the Technical Design Office (TDO) services required by ADS. The ADS TDO is responsible for:
   1. The Planning, Design and Build of the Platforms and infrastructure underpinning the AHE (private cloud), JSF (public cloud) and MODcloud (Defence public cloud) to meet the anticipated requirements of Army and wider Defence.
   2. Acting as the Design Authority of the Systems. Work alongside the Support Service teams to maintain and support the Private cloud infrastructure and the public / hybrid cloud platforms on which ADS delivered applications and services run.
   3. Ensuring that the AHE and JSF are secure and accreditable systems (with respect to MOD CyDR and the relevant JSPs).
   4. Providing 3rd/4th line support for the in-service AHE and JSF infrastructure and platforms.
2. ADS TDO is **not** responsible for the development of the software applications that run on the public / private clouds. Nor is it responsible for the delivery / build of websites delivered by ADS. The ADS TDO will focus on the delivery of technical capability (outcomes) that enables other parts of ADS to deliver / build live applications and the associated websites that may be required.
3. This document is split into three schedules:
   * 1. The technology utilised.
     2. The services required.
     3. The service levels required.

# Background

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. This includes elements from 605 Signal Troop (10 Signal Regiment) that directly support ADS. This figure increases when new products are in delivery.
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 JSF capability and is currently provided under a G-Cloud 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). In addition to these hosting capabilities, some aspects of the Continuous Integration / Continuous Delivery (CI/CD) pipeline for delivery onto both the JSF and AHE are in Microsoft Azure, enabling remote access to the product teams.

# **The Army Hosting Environment (AHE)**

1. The AHE is a ‘private cloud’ located on MOD premises, across two sites. It currently supports 120+ 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 Defence Information Infrastructure (DII) at Secret and MODnet at Official-Sensitive.
2. 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 100+ live application services on the Official-Sensitive, of which 50+ are Oracle APEX, 10+ are .Net; 2 utilising Software AG technology 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. 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. 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).
3. ADS is 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.
4. 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 apps and services that bridge security domains.

# **The Joint Server Farm (JSF)**

1. The JSF is a ‘public cloud’ currently hosted by Rackspace and is contracted as IaaS. The JSF provides the hosting capability for the Defence Gateway (DGW) that support 270,000 registered users across regulars, reserves, families, veterans and contractors. Application users access the DGW applications from all standard internet based devices (personal laptops, tablets, phones, etc.) but can also access them from the military WAN via the MOD Border Protection Service (BPS). It also provides Defence with a platform to host other capabilities, these include Defence Learning Environment (DLE) and Westminster (Cadet information system) amongst the 19 partners. The DGW provides an official capability that is accessed via Single Sign On (SSO) and Two Factor Authentication (2FA). Behind this are some 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 provide utilising PaaS and the DGW SSO.

# Operating Model

1. 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 both the AHE and the JSF, maintaining common technologies where possible.
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.
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.

# ADS Organisation, roles and responsibilities

1. The structure of ADS and 605 Signal Troop is detailed in the diagram and paragraphs below.

A picture containing diagram

Description automatically generated

1. **Product Teams.** These are based predominantly on a 6-person team, comprising of 2 developers, 2 testers, Business Analyst (BA) and Scrum Master 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.
2. **In Service Development Team.** These consist of 3 Oracle APEX and 2 .Net Developers supported by 3 matrix managed testers. This team enables the Service Managers to make changes to the services they support. They 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 with automated release on to production.
3. **Test.** ADS has testers embedded in the product and in service management teams. These testers are responsible for the automation of the functionality, installation 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 an environment as representative of the production environment as possible; on SIT, integration and exploratory testing are conducted; as well as the assurance of the automation tests.
4. Technical Assurance Service (TAS). The TAS Team ensure ADS strategies, processes and policies are applied throughout project delivery, QA test scripts & code, review ADS tooling and framework, research into future technology and following best practices.
5. **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 thus ensuring the use authoritative data.
6. **Defence Gateway Team.** This is a small DevOps 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 Rackspace.
7. **Network Operations Centre (NOC).** A team of predominantly military (from 605 Troop) personnel that monitors and supports the AHE. 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.
8. **Security Operations Centre (SOC).** A mixed team of civil servants, military and contractors that provide monitoring of event feeds and generate alerts for unexpected events / logons etc.
9. **Service Desk.** A team of civil servants and military that provide the first line of support for applications.
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.
11. **Army Data Analytics Team (ADAT).** Develop & maintain digital dashboards for Army.
12. **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 and 4th line support for these services, predominately infrastructure and main core services for the data centres.
13. **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.
14. **Compliance Team.** Ensure ADS adheres to security and policies as laid out in Joint Service Publication (JSP) 440 and 604, ISO 27001 and security architecture.
15. **Configuration Team.** Responsible for the configuration control of hardware, software and documentation.

# Schedule 1 –Technology

1. These are the key technologies that underpin the platforms and applications used within the AHE and JSF. The service provider and the resource they place 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.
2. Server Infrastructure.

|  |  |
| --- | --- |
| Compute | Relevance |
| The AHE currently uses Cisco UCS servers, Blades and Chasses to provide its compute capability. | The majority of server infrastructure is virtualised with limited exceptions e.g. a SAS HADOOP Cluster. |

1. Network Management

|  |  |
| --- | --- |
| Networking | Relevance |
| As well as the VMware 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.  Infoblox is utilised for IP Address Management (IPAM) and integration with vRA.  Cisco Meraki MX Appliances, MR Access Points and Cloud managed Switches. | The base position used is a zero trust configuration (i.e. total platform isolation). All access then needs to be explicitly specified and understood. Load balancers are provisioned on a per platform basis utilising NSX-T Edge services gateway LLB features. |

1. 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 vSAN | vSAN is currently only used on a small segment of the system. |

1. VMware Virtualisation and Management Technologies.

|  |  |
| --- | --- |
| VMware Products | Relevance |
| vCloud Suite to include;  ESXi  vCenter  vRealize Automation  VRealize Business  VRelize Operations  NSX-T  Site Recovery Manager | The AHE and JSF are both Software Defined Data Centres (SDDC). |

1. Operating systems.

|  |  |
| --- | --- |
| Operating Systems | Relevance |
| RedHat Linux 6.x / 7.x /8.x  Microsoft Server 2012 R2 / 2016 /2019 | All ADS platforms are built using scripted installs onto hardened versions of these operating systems that are the responsibility of the team to deliver and maintain. |

1. 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 Business Intelligence EE  Oracle BI Publisher  Oracle APEX and ORDS  Oracle Fusion middleware  Oracle Data Vault, VPD and TDE  Oracle Warehouse Builder  Oracle Data Integrator  Oracle Enterprise Manager | Key elements of the ADS Oracle platform reference architecture. |

1. Microsoft System software.

|  |  |
| --- | --- |
| Microsoft Software | Relevance |
| AD  ADFS  SharePoint  SQL Server  Reporting Services  CRM Dynamics  Team Foundation Server (Azure DevOps)  Azure Stack  Azure  Release Management  IIS  SCCM  SCOM | Key elements of the ADS Microsoft Application Platform reference architecture. |

1. The following SAS products are used:

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

1. 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 Kerberos (with a possible future move to OpenId Connect). |
| JSF standard authentication | The DGW in the JSF is a SAML2-based authentication and SSO system. This is based on Microsoft AD FS. | The SSO between the user and JSF web based applications is provided by the DGW. The applications on the Oracle Platforms connect to the DGW using SAML2 (with a possible future move to OpenId Connect). |

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

|  |  |  |
| --- | --- | --- |
| Automated application delivery | | Relevance |
| 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 the all platforms and integration troubleshooting will be required. |
| Performance Testing | Micro Focus LoadRunner |  |
| AV and Anti-Malware | ADS primarily use McAfee ePO, MOVE and MS defender. |  |
| 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. |
| Integration and Release | The integration and delivery of application code artefacts is supported using Microsoft Team Foundation Server / Azure DevOps and Jenkins. | **Peripheral relevance to this service**. These applications will interact with the Oracle and Microsoft platforms and integration troubleshooting will be required. |
| Source control | All software is loaded into TFS/GIT | All source (e.g. configuration scripts) must be loaded into Git. |
| Containerisation and Orchestration | Pivotal Cloud Foundry, Docker and OpenShift. | technologies under evaluation to provide cloud-native PaaS. |
| KMS | Gemalto Key Management | Centralised Keys Manager for encryption at rest. |
| Password Management | The 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 to support the Technical and Security Architecture and provide evidence to meet JSP 604 and Compliance/Accreditation requirements. |
| Hardware Security Module (HSM) | Thales – Ncipher PCI-E and SafeNet appliances | Used to store the private keys for the PKI solution |
|  |  |  |

1. All platform configuration changes are undertaken using automation.

|  |  |  |
| --- | --- | --- |
| Automated system software delivery | | Relevance |
| Automated delivery | ADS uses Red Hat Ansible, vRealize Automation and Orchestrator for the automated delivery of changes to the system software underpinning a Infrastructure and System Software components. | 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. |
|  |  |  |

1. Security Monitoring.

|  |  |  |
| --- | --- | --- |
| Security Incident Event Management | | Relevance |
| SIEM | The AHE utilises ArcSight as the Security Event Management (SIEM) System. | All Infrastructure and Platforms are configured to provide syslog or CEF formatted security logs to the ESM and Logger. |

1. Proactive Monitoring.

|  |  |  |
| --- | --- | --- |
| Proactive Monitoring | | Relevance |
| Monitoring | Solarwinds NPM & SAM network, system and platform health and availability.  HP OneView – Monitors the Compute tier for health and provides centralised management and patching of the blade system.  Cisco Data Center Network Assurance and Insights suite  Cisco Intersight Cloud Operations Platform  vRealize Operations provides centralised reporting and health monitoring of both physical and virtual infrastructure. Supports Show back/Charge back cost model.  Oracle Enterprise Manager  Splunk | Key tools for system monitoring and support |

1. Large 3rd Party Capabilities.

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

# Schedule 2 – Services

1. The supplier must provide the services required to architect, design and build the Army Hosting Environment (Private Cloud) and Joint Server Farm (Public Cloud) across the hardware and software and specialist technical domains (listed above in Schedule 1) that are required to deliver a data centre capability (spanning two physical locations) to host application and services in Defence. The service will also need to provide the necessary skills and expertise to maintain, support and change the technical architecture and design of ADS digital ICT Cloud solutions including IaaS, PaaS and SaaS-based services using this technology. It must ensure technical architecture is secure and compliant with Defence policies and industry best practice. Individuals that fulfil this requirement MUST hold Security Check (SC) as a minimum. Those with regular access to the server rooms or requiring a high degree of privilege across the system must hold Developed Vetting (DV).
2. The high-level deliverables for the service are:
   1. Provide and maintain a technical roadmap, architect, design and build solutions, formulate estimates and provide design expertise for new, and enhancements to existing, Infrastructure, platform and application services, based on the prioritised business requirements.
   2. Produce and review relevant technical design documentation to support the Infrastructure and application platforms and services.
   3. Provide ad hoc support to troubleshoot problems with Network, Infrastructure, Platforms and services within the hosting environments.
   4. Write and develop policies and standards for the Army and wider defence, and technically assure that all Infrastructure Platforms and services are aligned to the aforementioned policies and standards.
   5. Provide technical oversight for all designed and hosted applications and services.
   6. Provide expert advice and guidance to enable the Army to make informed decisions.
   7. Ensure that all solutions are hardened, technically secure and are Vulnerability Assessed and/or Penetration tested.
   8. Ensure that all solutions have the necessary integration with the ADS Security Operation Centre (SOC).
   9. Support the commercial viability of the hosting environments by deriving and operating appropriate cost models and charging processes.
3. The team will be required to work with other suppliers/strategic partner’s resources and internal staff to ensure a coherent delivery of service.
4. Initially ADS require a core team of resources to deliver the Technical Design Office service (TDOaaS). Table 1 provides a list of the minimum full-time equivalent (FTE) roles and corresponding SFIA and clearance levels the technical resources that deliver this capability will require. It will be the responsibility of the individual service provider to define the team structure they would utilise to deliver and maintain this capability as a service. The Authority will agree the outputs of the service monthly (in advance) and will hold the supplier to account for delivery of these outputs at the month end. Contractual levers exist to take action against the supplier for failure to deliver agreed outputs or resources, to appropriate timescales and quality.

Table 1 – Minimum FTE Resource Structure

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ser** | **Role Title** | **High Level Description** | **SFIA**[[2]](#footnote-2) **Level** | **Clearance** |
| 1 | Lead Technical Solutions Architect | Design Authority for all ADS owned and managed Systems. Responsible for the future technical direction of the AHE and JSF and the overall design of the current infrastructure and platform solutions. Needs to have both depth and breadth and demonstrable knowledge within all key technology areas. | 7 | DV |
| 2 | Deputy and Oracle Solutions Architect | Design Authority for all Oracle based Platforms and Services. Deputy Technical Solutions Architect. | 6 | SC |
| 3 | Microsoft SME Senior Solutions Architect | Design Authority for all Microsoft based Platforms and Services. | 6 | DV |
| 4 | Network - Infrastructure Architect | Design, Delivery and support of Network infrastructure that underpins the Cloud Infrastructure. | 5 | DV |
| 5 | Storage and Compute - Infrastructure Architect | Design, Delivery and support of storage, compute and Virtualisation solutions that underpin the Cloud Infrastructure. | 5 | DV |
| 6 | Oracle Technologies - Infrastructure Architect | Low Level Design and Build the Oracle Platforms and Solutions required. | 5 | SC |
| 7 | Linux/Unix - Infrastructure Architect | Design and delivery of the Secure Red Hat Linux O/S Platforms and Ansible automated delivery and update capabilities. | 5 | DV |
| 8 | Linux/Unix – DevSecOps Infrastructure Engineer | Building and maintenance of the Secure Red Hat Linux O/S Platforms and Ansible automated delivery and update capabilities. | 5 | SC |
| 9 | Microsoft - DevSecOps Infrastructure Engineer | Design, Building and maintenance of the Secure Microsoft O/S based Platforms across all ADS owned and managed Infrastructure. | 5 | DV |
| 10 | Public Cloud - DevSecOps Infrastructure Engineer | Domain expert in Public cloud service provision to MoD standards with a specific focus on AWS and Azure and System Administrator of the JSF. | 5 | SC |
| 11 | Technical Security Architect | Responsible for delivering technical Information Security services. This will include supporting the Information Security Information Management requirement for security governance, control, audit and security measures in support of Army HQ. | 5 | SC |
| 12 | Networks - Senior Cloud Infrastructure Engineer | Working alongside the Network Infrastructure Architecture to manage and maintain the Network, ACI Fabric, Firewalls, HSMs and Keys managers. | 5 | DV |
| 13 | Senior DevOps (Linux) Sys Admin | Working alongside the Linux/Unix Infrastructure Architect design, managing and maintaining solutions across both Private and Public clouds | 5 | SC |
| 14 | Security & Identity Architect | A Domain expert in PKI Solutions, HSMs, Keys and identity management. | 5 | DV |
| 15 | DevOps Automation Architect | Develop and the IaaS, PaaS, SaaS & XaaS offerings available for consumption via the Army’s Self Service Portal. An expert in Cloud Automation, DevOps tooling and Public cloud and container Orchestration. | 5 | SC |

1. The supplier is expected to provide resources that fit the indicated SFIA levels indicated above for ‘*Solution Development and Implementation’* or ‘*Strategy and Architecture’* and be able to justify them 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.
2. The supplier and the resources it provides must be free of any commercial ties or obligations to any hardware or software vendors.
3. The supplier will be required to provide a client interface to agree business prioritisations and deliverables.
4. Subject to demand and budget ADS require the ability to scale up and down the resource requirements. 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 monthly cost for the core capability.

# Scaling

1. ADS require confirmed rate cards for the provision of ‘add-ons’ or resources for a specific project or initiatives. This would involve the ability to select pre-defined service offerings that would be on and above the base capped core service, as these requirements would be separately funded by the project/business area(s).
2. The requirement for the provision of additional resources would take 2 forms:
3. Add a role - if an initiative requires a new set of skills e.g. a Technical Delivery Manager and solution Architect to support a customer’s delivery into the AHE.

Or

1. Duplicate a role - if there is need to scale up existing skills or provide an outcome e.g. Technical Reviews, Scoping Documents, Out of Hours support, Solution Design and Solution Implementation.

# Out of Hours Support

1. 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;
   1. Security Incident – Under Defend of the segmentation model incident response must be within 30 minutes of been identified. Once the SOC have carried out their initial investigation Technical advice may be required on suitable COA’s.

Or

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

# Schedule 3 – Service Levels

### Provisioning

1. The service supplier is expected to use their ‘best endeavours’ to provide resources to meet the priorities specified by ADS. Specifically:
   1. Provision of further resources within 30 calendar days.
   2. Exit of current resources no longer required within 7 calendar days.
2. 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.
3. If the supplier wishes to replace a resource that is currently delivering outputs, then if required the supplier must arrange a period of dual running for the new resource to come fully up to speed on the area and be able to provide seamless delivery of outputs. This period of “dual running” will be at the supplier’s expense and not charged to the Authority.

# Government Furnished Equipment (GFE)

### Licencing and Support Agreements

1. 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:
   1. Microsoft EA to include MSDN and Azure subscriptions.
   2. VMware ELA.
   3. Oracle Premier licence support.
   4. Oracle Advanced Customer Services.
   5. Red Hat standard support.
   6. HPe Support.
   7. Cisco SmartNet Support.
   8. Pure support.

### Hardware and Software Infrastructure Procurement

1. ADS will be responsible for procurement of all the IT assets and equipment required to support the AHE and the JSF. The Technical Design Office Team will be responsible for defining the technical requirements to ensure the correct equipment can be procured to meet the requirements of the business.
2. **Intellectual Property Rights (IPR)**. The selected supplier shall not retain IPR relating to any services, designs, documentation or configuration delivered during the terms of the contract.
3. **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.

**Duration**. The duration of the overall need is assessed as 24 months from award.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Column1** | **Lead Technical Solutions Architect** | **Deputy and Oracle Solutions Architect** | **Microsoft SME Senior Solutions Architect** | **Network - Infrastructure Architect** | **Storage and Compute - Infrastructure Architect** | **Oracle Technologies - Infrastructure Architect** | **Linux/Unix - Infrastructure Architect** | **Linux/Unix – DevSecOps Infrastructure Engineer** | **Microsoft - DevSecOps Infrastructure Engineer** | **Public Cloud - DevSecOps Infrastructure Engineer** | **Technical Security Architect** | **Networks - Senior Cloud Infrastructure Engineer** | **Senior DevOps (Linux) Sys Admin** | **Security & Identity Architect** | **DevOps Automation Architect** |  |  |  |  |  |
| SFIA Level required | 7 | 6 | 6 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |  |  |  |  |  |
| SFIA level for the supplied resource |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | | | |
| Minimum vetting level required | DV | SC | DV | DV | DV | SC | DV | SC | DV | SC | SC | DV | SC | DV | SC |
| Vetting level for the supplied resource |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Cisco UCS Servers, Blades and Chassis |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| As well as the VMware 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. Infoblox is utilised for IP Address Management (IPAM) and integration with vRA. Cisco Meraki MX Appliances, MR Access Points and Cloud managed Switches. |  |  |  |  |  |  |  |  | For each resource, confirm the skills that they have. The Authority will review the subject's CV to confirm that the assessment is justified.  Where a resource has 3 years demonstrable experience, enter 3Y in the relevant cell for that resource.  Where a resource has limited knowledge of a technology, enter L.  Where a resource has no knowledge of a technology, enter N. |  |  |  |  |  |  |
| Pure storage arrays |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Vmware vSAN |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| vCloud Suite to include; ESXi vCenter vRealize Automation VRealize Business VRelize Operations NSX-T Site Recovery Manager |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| RedHat Linux 6.x / 7.x /8.x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Microsoft Server 2012 R2 / 2016 /2019 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Oracle RDBMS  (including RAC, RMAN and ASM) Oracle Weblogic. (including SAML2) Oracle Access Manager (including Kerberos) Oracle Virtual Directory Oracle Internet Directory Oracle Business Intelligence EE Oracle BI Publisher Oracle APEX and ORDS Oracle Fusion middleware Oracle Data Vault, VPD and TDE Oracle Warehouse Builder Oracle Data Integrator Oracle Enterprise Manager |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| AD ADFS SharePoint SQL Server Reporting Services CRM Dynamics Team Foundation Server (Azure DevOps) Azure Stack Azure Release Management IIS SCCM SCOM |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SAS Viya/9.4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SSO/Kerberos/OpenId Connect |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SAML2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ADS uses the following toolsets for automated functional testing of applications and APIs. Mocha, Chai, Cypress, Javascript, Selenium/Java, F#/ Canopy |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Micro Focus LoadRunner |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ADS primarily use McAfee ePO, MOVE and MS defender. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 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). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The integration and delivery of application code artefacts is supported using Microsoft Team Foundation Server / Azure DevOps and Jenkins. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| TFS/GIT |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Pivotal Cloud Foundry, Docker and OpenShift. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Gemalto Key Management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Thycotic Secret Server |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Confluence / Jira |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Thales - Ncipher PCI-E and SafeNet appliances |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ADS uses Red Hat Ansible, vRealize Automation and Orchestrator for the automated delivery of changes to the system software underpinning a Infrastructure and System Software components. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The AHE utilises ArcSight as the Security Event Management (SIEM) System. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Solarwinds NPM & SAM network, system and platform health and availability |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| HP OneView – Monitors the Compute tier for health and provides centralised management and patching of the blade system. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Cisco Data Center Network Assurance and Insights suite |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Cisco Intersight Cloud Operations Platform |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| vRealize Operations provides centralised reporting and health monitoring of both physical and virtual infrastructure. Supports Show back/Charge back cost model |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Oracle Enterprise Manager |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Splunk |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ESRI ArcGIS Server Suite |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SAS – Statistical Analysis Software, Viya and Visual Analytics Suites |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Software AG Suite of technologies to include API Gateway, API Portal, Integration Server, Web Methods, Alfabet and ARIS. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Each resource must have a minimum of 7 years proven and demonstrable experience in the provision of the tehcnial solutions listed above. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resources must have proven recent and demonstrable experience (last 3-years) working in a large organisation supporting Agile methodologies to design/develop secure, scalable enterprise level application hosting platforms. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The actual resources that will be supplied must have a minimum of 6 Years proven and demonstrable experience as the Design Authority for large hosting environments or infrastructure projects. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have extensive, recent hands on knowledge and experience with the deployment, configuration and support of NVME based AFA’s to include Pure Storage FlashArrays and FlashBlades. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have extensive hands-on knowledge and experience with HPe-Proliant compute hardware, Cisco UCS servers, Cisco adaptive security appliances, Nexus switches, DeepSecure data-diodes, Enterprise Catapans and Gemalto-HSMs keys-managers. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have experience of delivering Enterprise PKI hosted solutions and running a Level 1 Certificate Authority (L1CA) service within a highly secure defence accredited environment. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The actual resources that will be supplied must have demonstrable experience within last 3-years of DevSecOps automation using Ansible and Ansible Tower to provision platform infrastructure as software. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have demonstrable experience within last 3-years presenting/briefing C-Level executives/influencers to support business cases and COAs. Requires the ability to deliver clearly and confidently unpalatable information. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resources must have demonstrable experience (last 3-years) of DevSecOps expertise building PaaS container technologies (Docker/Kubernetes) utilising market leading tools (Pivotal CloudFoundry/RedHat OpenShift) within a secure, Defence accredited hosting capability. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Extensive and demonstrable expert market knowledge of industry trends and emerging technologies. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resources must have demonstrable experience (last 3-years) of successfully building software defined hosting infrastructure that collect/manage personal and/or sensitive information with appropriate controls and protection in-line with JSP440/JSP480/JSP604. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The actual resources that will be supplied must have demonstrable experience within the last 5-years of delivering to Defence enterprise level standards and policies |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have demonstrated experience of leading the integration of large multi-tier COTs applications into a highly secure and current Defence hosted and accredited environments. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The supplied resources must have recent and demonstrable experience of delivering High Level and Low Level Solution Design documents based on Oracle, Microsoft, VMware and Red Hat technologies. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The actual resources that will be supplied must have proven and demonstrable experience delivering, managing and maintaining a secure Private Cloud within a defence or government network. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resource must have extensive recent demonstrable experience of designing/delivering secure multi-tier hosting platforms based on Windows/Linux OS (Windows 2012 R2/2016/2019, RHEL 6.x/7.x OS) into secure SDDC based environments. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| The actual resources that will be supplied must have minimum 4 years design and implementation experience of delivering solutions that include VMware NSX-v, SRM, vRealize Automation and vCloud suite. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resources must have proven recent experience designing/delivering a MicroFocus ArcSight software/appliance solution within a secure environment and using vulnerability scanning tools to diagnose security issues within system infrastructure. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Supplied resources must be poly-skilled SFIA level 5-7 Architects and Infrastructure Engineers with a minimum of 7-years domain experience in their specific areas (Oracle, Microsoft, VMware, RedHat, PureStorage and Cisco). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Demonstrable experience within last 3-years of successfully integrating systems via APIs, including on-premise and other cloud-based services. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Attachment 2 – Charges and Invoicing**

**Part A – Milestone Payments and Delay Payments – NOT APPLICABLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Milestone Description** | **Milestone Payment amount (£GBP)** | **Milestone Date** | **Delay Payments (where Milestone) (£GBP per day)** |
| M1 | *[insert description]* | *[insert amount]* | *[insert date as per Outline Implementation Plan]* | *[insert amount]* |
| M2 |  |  |  |  |
| M3 |  |  |  |  |
| M4 |  |  |  |  |
| M5 |  |  |  |  |

**Part B – Service Charges – NOT APPLICABLE**

|  |  |
| --- | --- |
| **Charge Number** | **Service Charges** |
| **[Service Line 1]** | |
| [e.g. SL1C1] |  |
| **[Service Line 2]** | |
| [e.g. SL2C1] |  |

**Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges to support CORE & AD-HOC Activities during the life of the Contract. T&S Costs are not applicable for both CORE & AD-HOC - REDACTED**

|  |  |
| --- | --- |
| **Staff Grade** | **Day Rate (£)** |
| Lead Technical Solutions Architect (SFIA 7) | £ |
| Deputy and Oracle Solutions Architect (SFIA 6) | £ |
| Microsoft SME Senior Solutions Architect (SFIA 6) | £ |
| Network - Infrastructure Architect (SFIA 5) | £ |
| Storage and Compute - Infrastructure Architect (SFIA 5) | £ |
| Oracle Technologies - Infrastructure Architect (SFIA 5) | £ |
| Linux/Unix - Infrastructure Architect (SFIA 5) | £ |
| Linux/Unix - DevSecOps Infrastructure Architect (SFIA 5) | £ |
| Microsoft - DevSecOps Infrastructure Engineer (SFIA 5) | £ |
| Public Cloud - DevSecOps Infrastructure Engineer (SFIA 5) | £ |
| Technical Security Architect (SFIA 5) | £ |
| Networks - Senior Cloud Infrastructure Engineer (SFIA 5) | £ |
| Senior DevOps (Linux) Sys Admin (SFIA 5) | £ |
| Security & Identity Architect (SFIA 5) | £ |
| DevOps Automation Architect (SFIA 5) | £ |
| **Supplier Personnel Rate Card for Calculation of Time and Materials Charges to support CORE & AD-HOC Activities during the life of the Contract for OUT OF HOURS (To include Weekends & Bank Holidays). T&S Costs are not applicable for both CORE / AD-HOC & Out of Hours – REDACTED** | |
| **Staff Grade** | **Hourly Rate (£)** |
| Lead Technical Solutions Architect (SFIA 7) | £ |
| Deputy and Oracle Solutions Architect (SFIA 6) | £ |
| Microsoft SME Senior Solutions Architect (SFIA 6) | £ |
| Network - Infrastructure Architect (SFIA 5) | £ |
| Storage and Compute - Infrastructure Architect (SFIA 5) | £ |
| Oracle Technologies - Infrastructure Architect (SFIA 5) | £ |
| Linux/Unix - Infrastructure Architect (SFIA 5) | £ |
| Linux/Unix - DevSecOps Infrastructure Architect (SFIA 5) | £ |
| Microsoft - DevSecOps Infrastructure Engineer (SFIA 5) | £ |
| Public Cloud - DevSecOps Infrastructure Engineer (SFIA 5) | £ |
| Technical Security Architect (SFIA 5) | £ |
| Networks - Senior Cloud Infrastructure Engineer (SFIA 5) | £ |
| Senior DevOps (Linux) Sys Admin (SFIA 5) | £ |
| Security & Identity Architect (SFIA 5) | £ |
| DevOps Automation Architect (SFIA 5) | £ |

**Part D – Risk Register – NOT APPLICABLE**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Column 1** | **Column 2** | **Column 3** | **Column 4** | **Column 5** | **Column 6** | **Column 7** | **Column 8** | **Column 9** | **Column 10** | **Column 12** |
| **Risk Number** | **Risk Name** | **Description of risk** | **Timing** | **Likelihood** | **Impact (£)** | **Impact (description)** | **Mitigation (description)** | **Cost of mitigation** | **Post-mitigation impact (£)** | **Owner** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**Part E – Early Termination Fee(s) – NOT APPLICABLE**

**Attachment 3 – Outline Implementation Plan – NOT APPLICABLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Milestone** | **Deliverables**  **(*bulleted list showing all Deliverables (and associated tasks) required for each Milestone*)** | **Duration**  **(*Working***  ***Days*)** | **Milestone**  **Date** |
| M1 | [Concept Design] | [Statement of Requirements  System/Application Specifications  Interface Specifications  Systems Testing Strategy  Implementation Strategy and Plan  Risk and Issues Management Plan  Outline Disaster Recovery Plan  Project Schedule  Service Management Plan] |  |  |
| M2 | [Full Development] | [Design Verification Reports  Design Validation Reports  Change Management Plan  System/Application Implementation Plan  Risk and Issues Management  Project Schedule  Service Management Plan] |  |  |
| M3 | [System User Testing] | [System Test Report  Risk and Issues Management Plan  Project Schedule  Service Management Plan  Defects Log  Final Inspection and Testing Report] |  |  |
| M4 | [User Readiness for Service] | [Training Plan  Risk and Issues Log  Implementation Plan  Operations Plan  Data Conversion & Cutover Plan  Project Schedule  Service Management Plan] |  |  |
| M5 | [Implementation] | [Implementation Plan  Training Scripts] |  |  |
| M6 | [In Service Support] | [Post Implementation Report  Data Conversion and Cut-Over Plan  Service Delivery Reports  Risk and Issues Log  Service Management Plan  Defects Log] |  |  |

**Attachment 4 – Service Levels and Service Credits**

**Service Levels and Service Credits**

1. **. CONTRACTS KPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to contractual evidence and formal tracking of service requests

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narrative / Caveats** |
| 1.1 Submit, or provide feedback to, all Invoices,  SoW,  Deliverables and  Acceptance Certificates accurately and completely within agreed timescales. | 1.1.a Timely invoicing | Invoice late days in the life of the contract will not exceed 5. | Number of days any invoice is delivered late. | Number of days any invoice has been overdue in the life of the contract |
| 1.1.b Assessment of submission | Assessment of the complexity of work to provide feedback to;   * statements of work, * Deliverables or * acceptance certificate will be undertaken.   If the work required to provide feedback for any item is identified as complex this will be notified to the authority within 1 working day. | The number of on-time assessments.  The number of late assessments. | Requests for feedback relating to any of the following; SoWs, Deliverables must be submitted through the agreed request mechanism. |
| 1.1.c Standard contractual feedback | Feedback to the following will normally be provided within 2 working days:   * Statements of Work * Deliverables * Acceptance certificates | The number of feedback tasks provided on-time.  The number of feedback tasks provided late. |
| 1.1.d Complex contractual feedback | Where the work to provide feedback is assessed as complex the following will be provided to the authority:   * Justification for assessment as complex * Timescales for response * Milestones in providing feedback * External dependencies for providing feedback | The number of complex feedback tasks provided on-time.  The number of complex feedback tasks provided late. |

**2. SERVICE GOVERNANCE KPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to governance of the service provided by the TDO management team

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narrative / Caveats** |
| 2.1 Act transparently while working with the buyer. | 2.1.a Timely submission of  Transparency  Reports | All transparency reports and draft templates of reports will be submitted on time and in the agreed format as per Attachment 10 (Transparency Reports) of the Order Form and Schedule 6 of the Call Off T&Cs. | The number of Transparency Reports (hereafter TRs) issued on time will be recorded.  The number of TRs issued late will be recorded.  The average number of days late of all TRs will be maintained as a KPI. |  |
| 2.1.b Review of transparency reports | Transparency reports will be reviewed for continuing suitability annually and the results of any review passed to the Buyer to approve changes as they see fit. | The number of Transparency Report reviews undertaken. |  |
| 2.2 Analyse resource allocation and provide  recommendations within monthly delivery reports/updates. | 2.2.a Workload by sub-team | Maintain a prioritised backlog of work to be done by sub-team which includes; tasks to be done, work estimates and a priority rating for each task. | The number of tasks in a sub-team backlog.  The number of tasks (and the estimated hours for those tasks) delivered by each sub-team. | Given sub-teams organised around core skill sets these metrics will highlight skill sets which are under-resourced. |
| 2.2.b Monthly report on workload | The Supplier will provide a monthly report showing the metrics for ‘Workload by Team’ and identifying under or over-resourcing of any given team. Given the poly-skilled nature of the Supplier’s resources this may be used to re-balance individuals between teams and ensure the backlog is equally distributed across all areas of effort. | The number of Workload Reports (hereafter WrkLRs) issued on time.  The number of WrkLRs issued late.  The average number of days late of all WrkLRs. |  |
| 2.3 Supply the required key resources and services meeting the agreed deliverables and contractual obligations. | 2.3.a Services list | Each service item that will be available to service users will be documented in a service list. Each service item will be documented as one of the following three service types; advisory, operational support and project. | The number of service items provided by the Supplier.  Failure to list a service item will be recorded as a service incident. The number of such incidents in the life of the contract. |  |
| 2.3.b Key skill risk | The Skills required to deliver each service item will be recorded against it in the service list. Service items which rely on 2 individuals or fewer will be highlighted as ‘vulnerable’. | The number of ‘vulnerable’ service items.    Failure to list a service item as vulnerable if it meets the criteria will be recorded as a service incident. The number of such incidents in the life of the contract. |  |
| 2.4 When flexing resource, commit to an SLA to supply new resource within 20 business days or less of the request. | 2.4.a Recruitment  time | Time taken at each stage of the recruitment process will be recorded. | The number of requests for new resource.    The time from each completed request from the Buyer being formally provided to the Supplier to the resource being available for work. | Where a request is provided, a resource recruited and notified as available to the Buyer but the Buyer cannot allow the resource to begin work for 30 days or more the request will be recorded as abandoned by the Buyer. |
| 2.5 Ensure all services it delivers are to the standard required. | 2.5.a Service item quality standards and timeliness | The services list will specify any quality standards for a given service item and any timescales which have been agreed for advisory or operations support service items. | Failure to meet the quality standards for a service item will be recorded as a service incident (performance). The number of such incidents in the life of the contract.    Failure to meet the timescales for a service item will be recorded as a service incident (performance). The number of such incidents in the life of the contract. |  |
| 2.5.b Quality review | All performance related service incidents will be reviewed on a monthly basis to identify the root cause of the incident. A schema will be developed for the classification of root causes. | The number of reviews of service incidents relating to service item performance.  The number of root causes of performance related service incidents. |  |

**3. KEY SKILLS AND SQEPS SKPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to the maintenance of key skills and an appropriate number of Suitably Qualified and Experienced Persons (SQEP).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narrative / Caveats** |
| 3.1 Add value to ADS business over and above the contracted services e.g. ensure our consultants remain current is  their specialist domain knowledge so they can advise ADS as to new ways of working in the future. | 3.1.a Training needs identification | The Supplier will ensure that any training requirements to allow the continued support of the Buyer’s technical ‘stack’ are identified a training need requirement raised. | The number of identified requirements for training. |  |
| 3.1. b Maintaining  the requisite skills pool | Where a training requirement relates to an existing service item and there has been no change of the underlying technology the Supplier will ensure that members of the team acquire the requisite skills to fulfil the training need. | The number of requirements for training addressed by the Supplier as ‘within skill base’. |  |
| 3.1.c Adding new  skills | Where a training requirement relates to a new service item or new technology the Supplier will provide details of the training requirement to the Buyer and costed options for fulfilling it. | The number of requirements for training raised to the Buyer as ‘outside skill base’. |  |
| 3.1.d Transferring skills | Where the Supplier identifies the ability for it’s staff to provide training based on their skill-sets which will support training requirements of the Buyer’s personnel they will offer to add this training to their service list. | The number of offer to add a training service item to the service list.  The number of training service items added to the service list. |  |
| 3.2 Manage its resource skill against the contracted outcomes addressing any issues appropriately. | 3.2.a Team rebalancing | Where indicated by work undertaken for the ‘Workload by sub-team' and ‘Monthly report on workload’ KPIs the team will be rebalanced to support the work requirements to meet the contracted outcomes. | A log of ac=on taken to rebalance the team included re-assignment of individuals or responsibilities within sub-teams. |  |
| 3.3 Ensure its resources perform to the required standard. | 3.3.a Monitoring | The Supplier will monitor all service complaints and service item performance incidents to identify any issues relating to the professional performance of its’ resources. Where poor performance is indicated the Supplier will record a sub-standard performance issue and will grade them by a severity schema. | The number of issues relating to substandard performance by a supplier resource. |  |
| 3.3.b Discipline and training | Where sub-standard performance is deemed to be the result of the conduct of one or more members of the Supplier’s team appropriate disciplinary or re-training measures will be taken. | An anonymised record of numbers and types of training and disciplinary action taken. |  |
| 3.3.c Process improvement | Where sub-standard performance is deemed to be the result of poor process remediation actions will be identified. | A record of numbers and types of remediation actions taken. |  |
| 3.4 Provide replacement personnel to support the service as required minimising impact to the service operations. | 3.4.a Recruitment | Each requirement for replacement personnel due to the exit of a team member will be logged. | A record of each loss of available worker time (includes loss of FTE or significant down-grade of available working hours) the approach for replacement, timeliness of replacement and success or failure. | The Supplier will note and raise any contributing factors against each significant loss of ‘available worker time’ that relate to the Buyer’s conduct or working environment. |

1. **CONTINUAL SERVICE IMPROVEMENT KPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to the maintenance of key skills and an appropriate number of Suitably Qualified and Experienced Persons (SQEP).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narra4ve / Caveats** |
| 4.1 Subject to request by the Authority, conduct service reviews/ assessments of all operations across ADS, in line with ADS’ Vision, Strategy and Key  Principles to add value over and above the provision of resource. | 4.1.a Service review | Apart from the continuous review mechanisms that are incorporated by design to the KPI and SLA structure set out in this document the Supplier will conduct a full service review leading to suggested changes in the service design, service plan, individual service items, Supplier team structure, subteam composition or allocation of service item responsibility to subteams. | The number of requests for a full service review.  Continuous improvement metrics for each service item and listed against each KPI. | Full service reviews will be recorded as an item in the Service List and will leverage ISO27000 as a baseline standard. |
| 4.1.b SLA review | The Supplier will conduct SLA review quarterly as per the requirements in the T&Cs. | Number of quarterly SLA reviews conducted on time (within 30 days of the commencement of the next quarter).  Failure to conduct an SLA review will be recorded as a service incident. The number of such incidents in the life of the contract. |  |
| 4.2 At the request of the authority run quarterly review workshops to identify CSI opportunities. | 4.2.a Continual service improvement reviews | The Supplier will run service improvement reviews as requested by the authority and will leverage continual improvement SLAs, KPIs and metrics set out in this document to ensures they are effective. New metrics will be identified and added at Service Improvement Reviews. | The number of new SLAs, KPIs and metrics added to the SLA framework. |  |

1. **CAPABILITY (ADS’S “RAG” ASSESSMENT CRITERIA) KPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to the professional services and the technical capability that will be available for use by the Buyer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narrative / Caveats** |
| 5.1 Develop new functionality, or enhancements, against user stories and their acceptance  criteria in line with the estimates provided during relevant Agile planning sessions. | 5.1.a Project metrics | The Supplier will create and maintain a  framework for managing work requests which do not relate to established service items but which are project-based. Project management services will be included in the Supplier service list as Advisory services. | The number of requests for all types of project work by type.  Variation in delivery dates against estimated delivery dates.  Days of delay by reason. |  |
| 5.2 Commit to investigating and handling incidents and problems in line with ADS’s extant resolution, change timings and SLA’s for the applications and services in its service portfolio. | 5.2.a Incident  management | A number of ‘Incident Support’ service items will be included in the services list with associated timelines and quality guidance. | Service item KPIs for these service items will be recorded and reported on in the same way as all other service items in the services list. |  |

1. **DELIVERY KPIS AND SLAS**

Service Level Agreements and Key Performance Indicators relating to delivery of the services to be provided. Delivery is sub-divided into the three principal service types; advisory, operational support and project work.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLA** | **KPI name** | **KPI commitment** | **Metrics** | **Narrative / Caveats** |
| 6.1 Ensure the correct level of technical advice is provided to empower the authority to make informed technical decisions | 6.1.a Logging advice requests | The supplier will ensure that all requests for technical advice are logged and formally managed through an agreed workflow. | The number of requests for technical advice. | Requests for technical advice must be received though  the agreed request mechanism |
| 6.1.b Request for  Advice (hereafter  RfA) resolution  timescales | RfAs will be resolved as per the process set out below for all technical and assurance advice (hereafter Technical Advice Notes abbreviated to TcANs). | Metrics for RfAs will be part of the overall metrics for TcANs. |  |
| 6.2 Ensure all technical and assurance advice is objective and promotes a one team ethos to delivery | 6.2.a Formal assurance process | Requirements for technical and assurance advice will be logged and provided through an auditable process. | The number of requests for TcANs. |  |
| 6.2.b Proactive raising of TcANs | The supplier will proactively raise TcANs (including RfAs) that the authority cannot trigger because technical expertise to identify the need for advice. | The number of requests for technical advice raised proactively by the TDO team. |  |
|  | 6.2.c Triaging TcANs - including RfAs | TcANs will be triaged within 1 working day of receipt and will be assigned to a relevant resource in respect of; SFIA and technical knowledge.  TcANs will be triaged as Standard or  Complex. If a TcAN is triaged as  Complex an expected comple=on date will be provided as part of the triage process. | The number of TcANs triaged.  The number of TcANs triaged late.  The numbers of TcANs triaged as standard and complex.  The average number of working days to expected comple=on date of complex TcANs. | Requests for TcANs without sufficient information will be rejected at this point. Rejection of an incomplete request will be considered fulfilling the response timescale |
|  | 6.2.d Timescales for providing standard TcANs (including standard RfAs) | Standard TcANs will be completed within 5 working days. | The number of standard TcANs issued on time.  The number of standard TcANs issued late. | Changes to a TcAN once work has started will cause a new identical TcAN to return to triage and the existing TcAN will be recorded as a successfully completed TcAN. |
|  | 6.2.e Timescales for providing complex TcANs (including complex RfAs) | Complex TcANs will be completed by the completion date set during the triage of the TcAN request. | The number of complex TcANs issued on time.  The number of complex TcANs issued late.  The average number of days late of all TcANs. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 6.2.f Review of feedback | All TcANs provided will be reviewed by either a TDO sub-team leader of a member of the TDO management team. | See ‘Breach of process’ for relevant metrics |  |
| 6.2.g Log of assurance feedback provided | A log of assurance feedback will be maintained and the feedback will be retained for the dura=on of the contract to allow review if required. | The number of TcANs issued in the life of the contract.    Records of work done to issue each TcAN will be logged and any failure to do so will be recorded as a service incident. |  |
| 6.2.h Breach of process | TDO will maintain a log of assurance feedback provided outside the process. | The number of violations per month and over the course of the contract. |  |
| 6.2.i Complaint process | A mechanism for service stakeholders to raise complaints about assurance feedback will be maintained and publicised for the dura=on of the contract. An anonymous complaint mechanism will also be provided but named complaints encouraged. | The number of complaints received, upheld and dismissed. |  |
| 6.2.j Review process | The review process will sample assurance feedback provided and will verify it meets the intent of the SLA statement. | See Metrics against “6.2.g Log of assurance feedback provided” |  |

**Attachment 5 – Key Supplier Personnel and Key Sub-Contractors**

### The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

**Part A – Key Supplier Personnel**

|  |  |  |
| --- | --- | --- |
| **Key Supplier Personnel** | **Key Role(s)** | **Duration** |
| REDACTED | Account Manager | Contract Period |
| REDACTED | Lead Solution Architect | Contract Period |

**Part B – Key Sub-Contractors**

| **Key Sub-contractor name and address (if not the same as the registered office)** | **Registered office and company number** | **Related product/Service description** | **Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period** | **Key role in delivery of the Services** |
| --- | --- | --- | --- | --- |
| Cloud Native Ltd | 20-22 Wenlock Road, London, N1 7GU  Registered: 11315114 | Delivery of TDO outcomes | 96% | Provision of resources to deliver outcomes |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Attachment 6 – Software – NOT APPLICABLE**

### The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

### The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

**Part A – Supplier Software**

The Supplier Software includes the following items:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Software** | **Supplier (if an Affiliate of the Supplier)** | **Purpose** | **Number of Licences** | **Restrictions** | **Number of Copies** | **Type (COTS or Non‑COTS)** | **Term/**  **Expiry** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Part B – Third Party Software**

The Third Party Software shall include the following items:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Third Party Software** | **Supplier** | **Purpose** | **Number of Licences** | **Restrictions** | **Number of Copies** | **Type (COTS or Non‑COTS)** | **Term/**  **Expiry** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Attachment 7 – Financial Distress**

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

**PART A – CREDIT RATING THRESHOLD**

|  |  |  |
| --- | --- | --- |
| **Entity** | **Credit Rating (long term)**  *(insert credit rating issued for the entity at the Commencement Date)* | **Credit Rating Threshold**  *(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3)* |
| ***Boxxe Limited*** | DUN & Bradstreet | 10 |
| ***Cloud Native Ltd*** | DUN & Bradstreet | 10 |

**Attachment 8 – Governance**

**PART A – SHORT FORM GOVERNANCE**

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

|  |  |
| --- | --- |
| Operational Board | |
| Buyer Members for the Operational Board | SO2 ADS Service Operations, Army D Info Commercial, D Info Finance |
| Supplier Members for the Operational Board | REDACTED and/or REDACTED |
| Frequency of the Operational Board | Quarterly for Contract Performance; Monthly for agreement of Statement of Work (SO2 ADS Service Operations only) |
| Location of the Operational Board | Until such time as COVID restrictions are lifted either by Skype or Microsoft Teams. When restrictions lifted at Army HQ, Andover |

**PART B – LONG FORM GOVERNANCE – NOT APPLICABLE**

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

|  |  |
| --- | --- |
| Service Management Board | |
| Buyer Members of Service Management Board (include details of chairperson) | Not Applicable |
| Supplier Members of Service Management Board | Not Applicable |
| Start Date for Service Management Board meetings | Not Applicable |
| Frequency of Service Management Board meetings | Not Applicable |
| Location of Service Management Board meetings | Not Applicable |

|  |  |
| --- | --- |
| Programme Board | |
| Buyer members of Programme Board (include details of chairperson) | Not Applicable |
| Supplier members of Programme Board | Not Applicable |
| Start date for Programme Board meetings | Not Applicable |
| Frequency of Programme Board meetings | Not Applicable |
| Location of Programme Board meetings | Not Applicable |

|  |  |
| --- | --- |
| Change Management Board | |
| Buyer Members of Change Management Board (include details of chairperson) | Not Applicable |
| Supplier Members of Change Management Board | Not Applicable |
| Start Date for Change Management Board meetings | Not Applicable |
| Frequency of Change Management Board meetings | Not Applicable |
| Location of Change Management Board meetings | Not Applicable |

|  |  |
| --- | --- |
| Technical Board | |
| Buyer Members of Technical Board (include details of chairperson) | Not Applicable |
| Supplier Members of Technical Board | Not Applicable |
| Start Date for Technical Board meetings | Not Applicable |
| Frequency of Technical Board meetings | Not Applicable |
| Location of Technical Board meetings | Not Applicable |

|  |  |
| --- | --- |
| Risk Management Board | |
| Buyer Members for Risk Management Board (include details of chairperson) | Not Applicable |
| Supplier Members for Risk Management Board | Not Applicable |
| Start Date for Risk Management Board meetings | Not Applicable |
| Frequency of Risk Management Board meetings | Not Applicable |
| Location of Risk Management Board meetings | Not Applicable |

**Attachment 9 – Schedule of Processing, Personal Data and Data Subjects – NOT APPLICABLE**

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

* + - 1. The contact details of the Buyer’s Data Protection Officer are:
      2. The contact details of the Supplier’s Data Protection Officer are:
      3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
      4. Any such further instructions shall be incorporated into this Attachment 9.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | [**The Authority is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:   * ***[Insert the scope of Personal Data for which the purposes and means of the processing by the Supplier is determined by the Authority]***   **The Supplier is Controller and the Authority is Processor**  The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with Clause 34.2 to 34.15 of the following Personal Data*:*   * ***[Insert the scope of Personal Data for which the purposes and means of the processing by the Authority is determined by the Supplier]***   **The Parties are Joint Controllers**  The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:   * ***[Insert the scope of Personal Data for which the purposes and means of the processing is determined by both Parties together]***   For the purpose of Clause 1.2 of the joint controller clauses the [insert either Buyer or Supplier] shall be the Party referenced and responsible for those matters set out in Clause 1.2(a)-(e). ***Insert for the purpose of Paragraph 1.2 of the joint controller clauses which Party (either Supplier or Buyer) shall be responsible for those matters listed in Clause 1.2(a) – (e), including whose privacy policy should apply i.e.***  **The Parties are Independent Controllers of Personal Data**  The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of*:*   * ***Business contact details of Supplier Personnel,*** * ***Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer’s duties under this Contract.*** * ***[Insert the scope of other Personal Data provided by one Party who is Data Controller to the other Party who will separately determine the nature and purposes of its processing the Personal Data on receipt.***   *e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer]* |
| Duration of the processing | ***[Clearly set out the duration of the processing including dates]*** |
| Nature and purposes of the processing | ***[Please be as specific as possible, but make sure that you cover all intended purposes.***  ***The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.***  ***The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]*** |
| Type of Personal Data | ***[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]*** |
| Categories of Data Subject | ***[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]*** |
| Plan for return and destruction of the data once the processing is complete  UNLESS requirement under union or member state law to preserve that type of data | ***[Describe how long the data will be retained for, how it be returned or destroyed]*** |

**Attachment 10 – Transparency Reports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Content** | **Format** | **Frequency** |
| Performance | Feedback from end customer | Stand-ups & Presentation | Monthly |
| Charges | Days, Roles, no of resources | Agreed Statement of Work | Monthly & Quarterly |
| Key Sub-Contractors | List of Key-Subcontractors | Stand-ups and Presentation | Monthly & Quarterly |
| Technical | Delivery to date, cost and no of resources | Stand-ups & Presentation | Weekly, Monthly & Quarterly |
| Performance management | Delivery to date, roles, no of days, and resources, cost | Presentation | Quarterly |

**Attachment 11 – Ad-Hoc Tasking Order Process Map & Form**

**AD-HOC TASKING ORDER PROCESS MAP AND INFORMATION**

Contractor provides a Firm Price for the additional requirement (no. of days & role, plus any T&S) on Part 2 and returns

Authority and Contractor work together to amend cost or scope of the requirement

Authority identifies additional requirement and completes Part 1

Authority approves/rejects Firm Price, returns Part 3

Within 2 working days

Repeat as

necessary to

agree terms of

work package

Contractor delivers requirements

Contractor provides invoice for

work to Authority

Authority draws down against Non-Guaranteed Ad-Hoc Tasking Value (AHTV)

Authority

Contractor

Joint / Both

within 1 working day

Approved

Rejected

Authority accepts/rejects requirement has been completed to an acceptable standard (*with justification for rejection)*

Accepted

Rejected

within 1 working day

*using Ad-Hoc Tasking Order Form (Call-Off Schedule 12)*

Each Tasking Order is a MAXIMUM value and is to be based on the Firm Priced Man-Day Rates detailed at Annex A.

Supplier to provide a detailed response on how they will deliver the outcome required.

No work shall commence until the Supplier is in receipt of the final Signed Tasking Order.

Once signed by all stakeholders the Authority will raise the necessary Purchase Order via CP&F. Upon completion of the Task and final invoices paid, the Authority will reduce (if necessary) the value of the Purchase Order to ensure unused funding is put back into the Non-Guaranteed Ad-Hoc Tasking Value (AHTV).

Due to the very nature of Ad-Hoc Tasking, Tasks can be cancelled at any time by the Authority. Amendments may be required which could extend the task on the basis that original technical requirement has not changed.

The Contract Terms and Conditions will support all Tasking Order Forms.

**AD-HOC TASK ORDER FORM – PART 1**

ORDER NUMBER: 001 (new number to be utilised for each additional Task)

CONTRACT No: 701576584 – DInfoCom/0175

TO: boxxe Limited

1. Please provide at PART 2 the details of the resources required to carry out the task described below.

2. TASK REQUIREMENT

To provide interim additional support to ………………………………….…………with effect from ………until……………

Tasks to include (more details are provided within the attached Statement of Requirement (Where applicable)):

1)

2)

3. Detailed Tasks and timescales are to be agreed with SO2 ADS Service Operations. Boxxe Limited are to report on a weekly basis to agree allocation of service priorities and risks in order to deliver services to meet contract requirements.

4. Resources: In accordance with the roles and rates within Annex A with support to be provided from existing or additional boxxe Limited resources.

5. Payment will be based on the approved monthly Statement of Work between the customer and ADS. To Note: No T&S costs are to be included if work is to be undertaken at the usual place of work. Any T&S will be in accordance with the Authority’s T&S policy, will be based on actual costs incurred and agreed with the Authority.

6. boxxe Limited are to complete PART 2 of this Tasking Order Form with proposed staffing profile (additional resource) and provide a detailed response on who they will deliver the outcome required.

7. LOCATION

8. PERIOD OF TASK…………………. subject to review thereafter.

SIGNATURE ……………………………………………

NAME ………………..…Authority’s Customer

APPOINTMENT ……………………………………………

CONTACT NO ………………………………………..….

**AD-HOC TASK ORDER FORM – PART 2**

**ORDER NUMBER:** 001 (new number to be utilised for each additional Task)

CONTRACT No: 701576584 – DInfoCom/0175

FROM: boxxe Limited

1. It is advised that boxxe Limited shall undertake the task detailed in PART 1 of this Order Form, within the timescale indicated, for the following MAXIMUM PRICE.

a. List of roles No of Days Rate Price

(as detailed in Annex A)

b. Travel Expenses (if applicable) No of Arisings Rate Price

c. Total MAX FIRM PRICE for the task (a+b) £

SIGNATURE ………………………………………………………………………..….

NAME ……………………………………………………………………………

APPOINTMENT ……………………………………………………………..………….…

TELEPHONE NO: ………………………………………………………………………….

DATE ……………………………………………………………………………

**AD-HOC TASK ORDER FORM – PART 3**

ORDER NUMBER: 001 (new number to be utilised for each additional Task)

CONTRACT No: 701576584 – DInfoCom/0175

TO: boxxe Limited

1. To be completed by SO2 ADS Service Operations (or nominated representative)

**DELETE EITHER A OR B AS APPROPRIATE**

A. The Maximum price offer to undertake Order Number 001 on Contract No 701576584 – DInfoCom/0175 is commensurate with the work involved.

The work should proceed at ……………Hours on……………………………

B. The Maximum price offer to undertake Order Number 001 on Contract No 701576584 – DInfoCom/0175 is not commensurate with the work involved.

SIGNATURE ………………………………………………………………………

NAME ………………………………………………………………………

APPOINTMENT ……………………………………..……………………………….

TELEPHONE NO: …………………………………………………………………….

DATE ………………………………………………………………………

2. In addition to the above confirmation, the following is to be completed by the Authority’s Commercial Branch.

**DELETE EITHER A OR B AS APPROPRIATE**

A. The Maximum price offer to undertake Order Number 001 on Contract No 701576584 – DInfoCom/0175 is accepted as an Ad-hoc Task.

B. The Maximum price offer to undertake Order Number 001 on Contract No 701576584 – DInfoCom/0175 is not accepted as an Ad-hoc task.

SIGNATURE ……………………………………………………………………

NAME

APPOINTMENT Army D Info Commercial

TELEPHONE NO: ……………………………………………………………………

DATE ………………………………………………………………………

**Attachment 12 – Monthly Statement of Work template**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Key Performance Indicators (TBA)**   |  |  | | --- | --- | |  |  | |  |  | | | | | | | | | | | |  |
| **Service xxx – Jan 2022 Deliverables** | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Days booked per role | | |  |  |  |  |  |
| **Ser** | **Task** | **Description/Deliverable** | **Timescale** | **Role A** | **Role B** | **Role C** | **Days used** | **Completion** | **Benefits delivered** | **Cost of task** | **% completed** |
| **1** |  |  |  |  |  |  | **0** |  |  | **£0.00** |  |
| **2** |  |  |  |  |  |  | **0** |  |  | **£0.00** |  |
| **3** |  |  |  |  |  |  | **0** |  |  | **£0.00** |  |
|  |  |  |  | 0 | 0 | 0 | 0 |  |  | £0.00 |  |

**Signatures and Approvals**

**Agreement of this SOW**

 BY e-SIGNING this Statement of Work, the Parties agree that it shall be legally binding on the Parties:

|  |  |  |  |
| --- | --- | --- | --- |
| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
| **Signature:** |  | **Signature:** |  |
| **Name:** |  | **Name:** |  |
| **Role:** |  | **Role:** |  |
| **Date:** |  | **Date:** |  |

**Attachment 13 – Statement Relating to Good Standing (PCR 2015)**

**The Statement Relating To Good Standing**

**Contract Title:** Provision of Technical Design Office (TDO)

**Contract Number:** 701576584

1. We confirm, to the best of our knowledge and belief, that ***boxxe Limited*** including its directors or any other person who has powers of representation, decision or control or is a member of the administrative, management or supervisory body of ***boxxe Limited*** has not been convicted of any of the following offences within the past 5 years:

* 1. conspiracy within the meaning of section 1 or 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA;

* 1. corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906;

* 1. common law offence of bribery;

* 1. bribery within the meaning of section 1,2 or 6 of the Bribery Act 2010; or section 113 of the Representation of the People Act 1983;

* 1. any of the following offences, where the offence relates to fraud affecting the European Communities financial interests as defined by Article 1 of the Convention on the protection of the financial interests of the European Communities:

* + 1. the common law offence of cheating the Revenue;
    2. the common law offence of conspiracy to defraud;
    3. fraud or theft within the meaning of the Theft Act 1968, the Theft Act (Northern Ireland) 1969, the Theft Act 1978 or the Theft (Northern Ireland) Order 1978;
    4. fraudulent trading within the meaning of section 458 of the Companies Act 1985, Article 451 of the Companies (Northern Ireland) Order 1986 or section 933 of the Companies Act 2006;
    5. fraudulent evasion within the meaning of section 170 of the Customs and Excise Management Act 1979 or section 72 of the Value Added Tax Act 1994;
    6. an offence in connection with taxation in the European Union within the meaning of section 71 of the Criminal Justice Act 1993;
    7. destroying, defacing or concealing of documents or procuring the extension of a valuable security within the meaning of section 20 of the Theft Act 1968 or section 19 of the Theft Act (Northern Ireland) 1969;
    8. fraud within the meaning of section 2,3 or 4 of the Fraud Act 2006; or
    9. the possession of articles for use in frauds within the meaning of section 6 of the Fraud Act 2006, or making, adapting, supplying or offering to supply articles for use in frauds within the meaning of section 7 of that Act;

* 1. any offence listed:

* + 1. in section 41 of the Counter Terrorism Act 2008; or
    2. in Schedule 2 to that Act where the court has determined that there is a terrorist connection;

* 1. any offence under sections 44 to 46 of the Serious Crime Act 2007 which relates to an offence covered by (f) above;
  2. money laundering within the meaning of section 340(11) and 415 of the Proceeds of Crime Act 2002;

* 1. an offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B, or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996;

* 1. an offence under section 4 of the Asylum and Immigration (Treatment of Claimants etc) Act 2004;

* 1. an offence under section 59A of the Sexual Offences Act 2003;

* 1. an offence under section 71 of the Coroners and Justice Act 2009;

* 1. an offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994; or

* 1. an offence under section 2 or 4 of the Modern Slavery Act 2015;

* 1. any other offence within the meaning of Article 57(1) of Public Contracts Directive –

* + 1. as defined by the law of any jurisdiction outside England and Wales and Northern Ireland; or

* + 1. created in the law of England and Wales or Northern Ireland after the day on which these Regulations were made;

* 1. any breach of its obligations relating to the payment of taxes or social security contributions where the breach has been established by a judicial or administrative decision having final and binding effect in accordance with the legal provisions of the country in which it is established or with those of any jurisdictions of the United Kingdom.

1. ***boxxe Limited*** further confirms to the best of our knowledge and belief that within the last 3 years it:

* 1. has fulfilled its obligations relating to the payment of taxes and social security contributions of the country in which it is established or with those of any jurisdictions of the United Kingdom;

* 1. is not bankrupt or is not the subject of insolvency or winding-up proceedings, where its assets are being administered by a liquidator or by the court, where it is in an agreement with creditors, where its business activities are suspended or it is in any analogous situation arising from a similar procedure under the laws and regulations of any State;

* 1. has not committed an act of grave professional misconduct, which renders its integrity questionable;

* 1. has not entered into agreements with other suppliers aimed at distorting competition;

* 1. Is not subject to a conflict of interest within the meaning of regulation 24;

* 1. has not been involved in the preparation of this procurement procedure which would result in distortion of competition which could not be remedied by other, less intrusive, measures other than exclusion from this procedure;

* 1. has not had a contract terminated, damages or other comparable sanctions taken as a result of significant or persistent deficiencies in the performance of a substantive requirement under a prior public contract, a prior contract, or a prior concession contract as defined by the Concession Contracts Regulations 2016;

* 1. is not guilty of serious misrepresentation in providing any information required by this statement.

* 1. has not unduly influenced the decision-making process of the Authority or obtained confidential information that may confer upon it undue advantages in the procurement procedure;

* 1. in relation to procedures for the award of a public services contract, is licensed in the relevant State in which he is established or is a member of an organisation in that relevant State where the law of that relevant State prohibits the provision of the services to be provided under the contract by a person who is not so licensed or who is not such a member;

* 1. has fulfilled its obligations in the fields of environmental, social and labour law established by EU law, national law, collective agreements or by the international environmental, social and labour law provisions listed in the Public Contracts Directive as amended from time to time (as listed in PPN 8/16 Annex C).

I confirm that to the best of my knowledge my declaration is correct. I understand that the contracting authority will use the information in the selection process to assess my organisation’s suitability to be invited to participate further in this procurement, and I am signing on behalf of my organisation. I understand that the Authority may reject my submission if there is a failure to provide a declaration or if I provide false or misleading information.

**Organisation’s name: boxxe Limited**

**Signed:**

REDACTED

**Name: REDACTED**

**Position: Chief Revenue Officer**

**Date: 29/08/2021**

**Attachment 14 – Expenses Policy**

UK Rail Travel

Standard Class must be selected

**Accommodation**

Service Mess

If your business travel has taken you onto a base and you need overnight accommodation, it may be that staying in the Service Mess is more cost efficient than a hotel; and should be consid­ered. All military personnel should refer to **JSP 752** Pt 2 Chapter 3 for occasions in which any other form of accommodation may be considered. For civilian staff, the availability and suitability criteria for Mess accommodation is being further developed and will be included in policy guidance shortly.

**Hotel**

All hotel bookings must be made using the **GBT Online Portal**.

Civilian staff must comply with the approvals processes (Chapter 2). Service Personnel must have both line management and budgetary written or verbal authority before making subsistence arrangements and should note that Night Subsistence (NS) is paid for an overnight absence where there is no suitable Service accommodation provision.

All staff must consult the MOD **capped hotel rates** for spend limits in each location. The Booking Service website will raise a warning if you select a hotel exceeding the capped rate. To proceed with such a booking, you must have line manager written approval of Band D/ OF2/OR7 or above (or locally delegated budget management staff).

Exceptional circumstances where you might exceed a cap rate include: the only hotel available; an overall saving; concern as a ‘lone traveller’.

**Travel & Subsistence**

Spend taxpayers’ money responsibly.

If in doubt about what to claim, seek advice from your line manager, budget manager, or from Unit HR/Admin Staff and/ or DBS – it is best to check before you commit to expenditure. Details for military personnel is in **JSP 752**, and for civilian staff in the **Policy Rules and Guidance**.

You cannot claim for alcohol purchased whilst undertaking business travel, either as part of a meal or consumed in isolation.

**Subsistence cost limits**: You can claim for actual receipted expenditure, within the subsistence limits detailed below, (**not** at a flat rate). You must obtain and retain itemised receipts for all claims. If you do not have a receipt you will need auditable line manager approval, e.g. by email, before you claim, and you must keep the approval.

Over 5 hours £5.00

Over 10 hours £10.00

Over 12 hours £15.00

Evening Meal £22.50 (overnight stay)

Breakfast\* £10.00

\* when not included in the hotel/B&B rate

Motor Mileage Allowance (MMA) – UK

There are a number of different rates which are related to UK vehicle travel:

* Motor Mileage Allowance (up to 10,000 miles) 30p per mile
* Motor Mileage Allowance (over 10,000 miles) 25p per mile
* Motorcycle 24p per mile
* Pedal cycle 15p per mile
* Passenger Supplement 3p per mile for first

passenger; 2p per mile for second and additional passengers

* Equipment Supplement 2p per mile (taxable)
* Excess Fares Allowance 30p per mile

**Home to Duty Liability**

The Home To Duty Liability (HTDL) is the travel cost incurred getting to/from your normal place of work. This should be deducted from expenses incurred when undertaking business travel to/from the home and a business location. This deduction does not apply to travel

between business locations.

Using a Private Vehicle is probably the easiest application. If you normally drive to work and use your vehicle for business travel, then your Motor Mileage Allowance claim should have a deduction commensurate with the normal mileage to work. So, if you normally travel 10 miles to/from your normal place of work (total 20 miles) and drive 30 miles to/from a

business location (total 60 miles), the claim should be reduced by 20 miles. This results in a net MMA claim of 40 miles. The deduction only applies to travel to/from the home and

business location; not between your normal work place and business location(s).

**Attachment 15 – Cyber Implementation Plan**

|  |  |
| --- | --- |
| **Contract Title:** | The Provision of Technical Design Office (TDO) |
| **MOD Contract Number:** | 701576584 (DInfoCom/0175) |
| **CSM Risk Acceptance Reference:** | RAR-67BRA888 |
| **CSM Cyber Risk Level:** | High |
| **Name of Supplier (to be shared with the MOD only):** | boxxe Limited |
| **Current Level of Supplier Compliance:** | Cyber Essentials Plus (SAQ-944979226); High |
| **Reasons why Supplier is unable to achieve full compliance:** | n/a |
| **Measures planned to achieve compliance/ mitigate the risk with associated dates:** | n/a |
| **Anticipated date of compliance/mitigations will be in place:** | n/a |
| **Current Cyber Essential Plus Certification No:** | IASME-CEP-001486 |
| **Expiry Date:** | 12 November 2021 |
| **Renewal certification to be issued to the Authority:** | Annually until expiration of the Contract |
| **Name:** | REDACTED |
| **Position:** | Account Director |
| **Date:** | 14 October 2021 |

**Attachment 16 – Supplier’s Response - REDACTED**

|  |  |
| --- | --- |
| **Name of Requirement:** | **Provision of Technical Design Office** |

**Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses**

**see separate documents: Call Off Terms and Conditions AND Alternative and Additional Clauses**

1. It is expected that a new supplier will supply a full team of circa 15 people for the handover period. These people must be fully versed in the technologies. This same team must deliver the required outputs at the start of the contract period. [↑](#footnote-ref-1)
2. Skills Framework for the Information Age - <https://www.sfia-online.org/en> [↑](#footnote-ref-2)