**Condition 46a - Statement of Requirement**

**Provision of Aircraft Document Reader and Associated Support for A400M and C-17**

**Table of Contents**

Background ………………………………...………………………………………………….…….……….… 2

Scope of Requirement …………………………………………………………………………….….………. 2

Documents ……………………………………..……………………………..………………….…..………… 3

Required Certification and Quality Assurance …………................…………………………..…………… 4

Communications & Contract Reviews …………………………………..……………..…………….……… 5

Assumptions ……………………………………………………………...…………..………………….…….. 6

Regulations and Standards ………………………………………………………...………………………… 7

Annex A – System Requirements ……………………………………………………………………....….. 10

Annex B – Support and Performance Requirements …………………..…………...………..…..……… 16

Annex C – Project Management SOW ………………………………..…………….....……..……………18

**Background**

1. Front Line (FL) crews and engineering staff require access to a library of several thousand aircraft operating, flight-planning, air safety, regulatory, operation/exercise and tactical documents, as well as notices which may be urgent and/or temporary from a wide range of sources including the Aircraft Document Set (ADS) and Technical Information Documentation (TID). Much of the content is common across the RAF or AM Fce, though certain documentation is specific to aircraft or section. Many documents contain references to other documents, which may be hyperlinked. Certain documentation is mandatory and may require explicit acknowledgement of receipt at an individual level, prior to clearance to fly or operate. As the wide range of documentation is constantly being updated, the management and distribution of these documents in an efficient way is a complex and constantly changing piece that responds to user requirements.

2. Electronic Flight Bags (EFBs) are now a minimum industry standard, based upon the intention to reduce the amount of paper documentation and improve the ‘human machine interface’ that best contributes to the most efficient and safe operating. Not utilising an EFB ignores current best aviation practice and demonstrates a considerable under-utilisation of an available product which can contribute significantly to platform flight safety.

3. Under contract with OCCAR, Airbus update and release the TID as a set of S1000D objects which include Data Modules (DMs) that contain Computer Graphics Metafile (CGM) illustrations on a quarterly basis. Upon release the EA reviews the TID and approves the data allowing release to Airbus Military UK to be updated within the systems.  Between the quarterly releases, ad hoc updates to the TID (Advance Change Notes (ACN)) are released and when approved by the EA are incorporated into the TID.

**Scope of Requirement**

4. RAF crews and engineers require a security accredited single platform system for the document handling, processing, assuring content, editing, publishing, distribution, viewing and hosting of ADS and TID in digital format up to Official-Sensitive classification. Each of these activities is governed by strict air safety procedures and regulations. The product must enable the documents to be categorised and managed in a method which maximises accessibility to information and minimises duplication of effort by the AM Fce where there is common content across aircraft platforms and Squadrons.

5. The product shall provide crews and engineers with the most up-to-date version of the document set, as it refreshes when connected to Wi-Fi/Cellular Services globally.

6. The documents are in various formats, such as Airbus Exchange, other XML formats used in aviation, complex PDFs containing high volumes of bookmarks and intra-document hyperlinks.

7. The library must be accredited for hosting export-controlled documentation, e.g. datasets subject to International Trade in Arms Regulations (ITAR) and Export Administration Regulation (EAR).

8. The system must be suitable for ground & air use and accessible through individual issue devices.

9. As well as standard operating conditions, where access is required on-station, access is also required while operating away from home base where connectivity and a power source may be infrequent or via poor connections, and by personnel who only have access to MODNet terminals.

10. The document reader application must comply with all UK MoD security and IT regulations and other UK laws and regulations, including Data Protection.

11. To ensure understanding of the Authority’s requirements the Authority intends to work closely with the Contractor in an open and transparent working arrangement.  The A400M construct is complex requiring many agencies access to the ADS and TID including FL crews, Engineers, Defence Equipment & Support Employees, MOD enabling organisations and contracted support agencies. Therefore, there is a requirement for crews to operate in deployed locations with limited connectivity and support.

12. This working arrangement is particularly relevant to the management of risk that could adversely affect the successful acceptance of the documentation.

**Documents**

13. The following documents shall be handled by the system.

|  |  |  |
| --- | --- | --- |
| **Document** | **Source Document format** | **Supplier activity** |
| ATLAS C MK 1 Aircraft Document Set1 | Airbus Exchange XML. | Structured, Managed |
| C-17 Aircraft Document Set | PDF (note high volume of bookmarks and hyperlinks). | Managed |
| RAF Operations Manuals | Plain text. | Structuring. Managed |
| RAF Document & Media library | All common file types including PDF, .doc, .docx, JPEG, MPEG, MP4, AVI, XLS etc. | Hosted |
| TID2 - Engineering | S1000D | Structured, Managed |
| TID - Maintenance | S1000D | Structured, Managed |
| TID - Repair | S1000D | Structured, Managed |
| TID - Associated Data | S1000D | Structured, Managed |
| TID - Logistic | S1000D | Structured, Managed |
| TID - Shop | S1000D | Structured, Managed |
| Aircrew Publications (AP)3 | PDF | Hosted |
| Instructions for Sustaining Type Airworthiness (ISTA)4 | MS Word | Structured.  Hosted |
| Aviation Engineering Orders and Local Procedures5 | PDF | Hosted |
| CAMO Procedures | MS Word | Structured.  Hosted |
| CAMO Technical Instructions | PDF | Hosted |

**Required Certification and Quality Assurance**

14. The Contractor is to comply with the relevant and current UK and EU legislation including but not limited to ISO 9001, and the Health and Safety (H&S) at work act.  All safety related materials including documentation, plans, certificates etc. shall be made available upon request for independent audit.

**Communications & Contract Reviews**

15. Unless agreed to the contrary, the Contractor is to facilitate progress meetings at the locations shown against each meeting in accordance with DEFCON 642.

The following meetings are to be held as a minimum:

1. Inaugural meeting within 2 weeks of contract award - Contractors premises or via TEAMS.
2. Quarterly Progress meetings – MOD facility/Contractors’ premises or via TEAMS.
3. Reviews, implementation discussions and other meetings required to fulfil the contract – MoD facility/contractor premises or via TEAMS.

**Assumptions**

16. The current AMF (Air Mobility Force) EFB device for all platforms is an iPad operating iOS.

17. In addition, A400M crews also require access to the ADS via DO provided MS Surface Pro EFBs that run its FlySmart+ software.

18. The software solution will remain accessible in line with operating system upgrades, for example iOS, Android, and Windows.

19. The solution will be intuitive to minimise impact of implementation and limit the changes required to internal authority procedures. The detail of the current process can be found in the A400M ADS Management Process (Appendix 1).

20. The day-to-day management will be undertaken by two authority personnel separated as engineering and operations and will be available to interact with the supplier.

**Regulations and Standards**

21. The service is to be provided in accordance with MRP regulation RA.

* RA 1005 – Contracting with Competent Organisations
* RA 1202 – Cyber Security for Airworthiness and Air Safety
* RA 1310 – Air System Document Set
* RA 2401 – Documents and Records
* RA 4809 – Acceptance of Components
* RA 5103 – Certification of Design
* RA 5406 – Aircrew Publications
* RA 5301 – Air System Configuration Management
* RA 5855 – Parts and Appliances
* RA 5890 - Cyber Security for Airworthiness and Air Safety – Type

Design and Changes / Repairs to Type Design

**Annex A – System Requirements**

|  |  |  |
| --- | --- | --- |
| **Serial** | **Requirement** | **A400M ONLY** |
| **1** | **Accessibility** |  |
| 1.1 | The system shall be fully hosted, including system and data, and shall not require any client installation on end user or administrator machines. |  |
| 1.2 | The system shall be remotely accessible via a wide range of commercially available systems and browsers (including but not limited to Windows, Edge, Safari, iOS etc). Accessibility must be in line with MOD policy for the classification of the documentation and any associated aggregation risk. |  |
| 1.3 | The system shall support publication of manuals and documents to mobile devices, including, but not limited to, latest versions of iOS, Android and Windows, via a readily downloadable application for offline access. |  |
| 1.4 | The system shall support publication of manuals and documents to web browser for online access via the internet and MODNet. |  |
| 1.5 | All documents shall be viewable within the same application8/web browser. |  |
| 1.6 | The System must be compatible with iOS and other operating systems such as Windows or Android.9 |  |
| 1.7 | Following offline access, and on connection to wi-fi/cellular services globally, the system shall refresh and update to the latest document versions. |  |
| 1.8 | Users shall be able to export documents and individual pages of a document in a pdf format. |  |
| **2** | **Interface characteristics** |  |
| 2.1 | All systems, applications and interfaces, including those for administrators, should have a modern and consumer grade look and feel, and should be intuitive to use with minimal training required. |  |
| 2.2 | The system shall give users the ability to adjust visual and usability settings, including night mode (for night flying) and the ability to adjust app font sizes and font sizes for structured content. |  |
| 2.3 | The user shall be able to zoom in and out of content which cannot be resized (e.g. images, pre-formatted PDFs). |  |
| 2.4 | Images and text shall be viewable at the same resolution as the source document. |  |
| **3** | **Navigation** |  |
| 3.1 | Features of structured documents shall be available to users when viewing documents (including but not limited to dynamically filtering by serial number; toggleable layers need-to-know/additional info/regulatory info; revision highlights; graphic hotspots; collapsible checklists; etc). |  |
| 3.2 | Hyperlinks between documents within the library shall work and shall update when new revisions of documents are released without manual intervention. |  |
| 3.3 | The user shall be able to filter their library by metadata filters (e.g. aircraft type, operation type, document type, role). |  |
| 3.4 | The user shall be able to navigate their library in multiple ways according to their use case, including but not limited to the table of contents, quick links, and search. |  |
| 3.5 | The System shall have a search function, which shall search within areas including but not limited to the content of documents, document metadata and titles (either within an individual document or across all documents within the whole library). |  |
| 3.6 | The user shall be able to add personal annotations. Annotations shall be synced across a user’s profile (app and web browser access) and they shall not be lost when a new revision of a document is released. |  |
| **4** | **Administration** |  |
| 4.1 | There shall be no limit to the number of administrators the MOD can allocate. |  |
| 4.2 | Administrators shall have the ability to issue new revisions of the same document without losing metadata related to that document. |  |
| 4.3 | An auditable history of each document update should be viewable. |  |
| 4.4 | Administrators shall be able to apply metadata to documents within the library to facilitate management of a complex library. |  |
| 4.5 | Administrators shall be able to make changes to the library layout, folder/group structure and document order as required at any time. |  |
| 4.6 | There shall be no system limit to the number of folders/groups or number of documents within the library |  |
| 4.7 | Administrators shall be able to make bulk changes to the library layout and folder structures of live data. |  |
| 4.8 | Administrators shall be able to schedule automatic publication/effectivity of documents or folders/groups based on UK dates/timecodes. |  |
| 4.9 | Administrators shall be able to configure users, groups, and roles without intervention from the Supplier. |  |
| 4.10 | There shall be no limit to the number of users, groups and roles that can be created. |  |
| 4.11 | There shall be permissions-based access to data to the level of individual documents and administrative functions. |  |
| 4.12 | Administrators shall be able to select from a number of install options including, mandatory manual download, mandatory automatic download or optional download. |  |
| 4.13 | There shall be metadata functionality within each document that allow the administrator to apply read and sign requirements to individual and/or multiple user groups at a document level. |  |
| 4.14 | Administrators shall be able to restrict access to controlled material (e.g. ITAR/EAR material. DEFCON 528 and JSP 248). |  |
| 4.15 | External parties shall be able to be granted permission to access material for printing updates to manuals.10 |  |
| 4.16 | There shall be the facility to assign metadata to each document, including but not limited to, Document Owner, Document Owner Contact Detail, Document review/expiry dates, Document Source (Primary or Secondary with link to document source location for secondary (http, SharePoint, ALaRMS etc). |  |
| 4.17 | There shall be the ability for administrators to generate new metadata fields. |  |
| 4.18 | There shall be the facility to assign individual system users and/or role groups as Document Managers within the metadata of each document. |  |
| 4.19 | There shall be associated automated notifications to Document Managers if a document exceeds its review or expiry period. |  |
| 4.20 | There shall be the functionality to allow each user and/or role group to see a list of documents for which they have been designated as Document Managers. |  |
| 4.21 | There shall be the functionality to allow administrators to see a list of documents for which each user and/or role group have been designated as Document Managers. |  |
| 4.22 | There shall be the functionality for administrators to build intuitive Forms within the System using standard form building selection options (text fields, checkboxes, select boxes, radio buttons, etc) and publish these forms to the document library to enable users to submit data to pre-selected administrators via automated email (both online and offline). |  |
| 4.23 | Submitted forms should be available in a repository to view at any time. |  |
| 4.24 | End users shall have the functionality to highlight areas of text or chapters within all documents in the System and submit comments to administrators for review of specific document concerns. |  |
| 4.25 | The System should allow administrators to define parameters for automatic generation of email notifications to designated administrators based on pre-selected documents metadata/metrics. |  |
| **5** | **Interaction** |  |
| 5.1 | The System shall be fully integrated and allow all users to easily carry out their tasks with only a minimum of training and support. |  |
| 5.2 | The System will be sufficiently matured to allow for a high-quality user experience at every stage. |  |
| 5.3 | The System shall allow easy comparison between new DO ADS and TID data, existing DO ADS and TID data and existing UK Nationalised ADS and TID data. | X |
| 5.4 | The System shall allow selection of DUs/DMs from either new DO ADS and TID data, or existing DO ADS and TID data or existing UK Nationalised ADS and TID data to create a revised nationalised ADS and TID. | X |
| 5.5 | The System shall allow temporary revisions or additional supplements to be added to any document including the ADS and TID without the need for removal or republishing of the original ADS and TID data/document. | X |
| 5.6 | The System shall allow editing of all ADS and TID data. | X |
| 5.7 | The System shall allow the creation of structured, managed customer manuals. |  |
| 5.8 | The System shall allow editing of all customer structured, managed data. |  |
| 5.9 | The system shall allow the customer to review draft content in pdf, a mobile app (currently iOS) and LPCNG/Fly Smart+ formats and approve/reject and comment on any changes. |  |
| 5.10 | The System shall publish all documents in multiple formats.11 |  |
| 5.11 | The System shall provide a delta report of changes on release of updated versions of the TID. |  |
| **6** | **Data Transmission** |  |
| 6.1 | The System shall update documents utilising minimum data transfer to limit bandwidth required on Wi-Fi and cellular networks, increasing performance, and keeping data cost issues to as low as practicable. |  |
| 6.2 | The System shall allow access to documents utilising minimum data transfer to limit bandwidth required on Wi-Fi and cellular networks, increasing performance, and keeping data cost issues to as low as practicable. |  |
| 6.3 | All data held on the application shall be available to the users offline. |  |
| 6.4 | On connection to wifi and cellular networks, automated processes shall initiate to ensure data integrity, not limited to corrupted, missing or out of date data, on the application. |  |
| **7** | **Control and Revision Marks** |  |
| 7.1 | It must be possible to watermark all documents that have not been released for use on the aircraft by the customer as DRAFT or NOT FOR OPERATIONAL USE. There must be no potential for confusion between DRAFT and live documents on the system and once downloaded. |  |
| 7.2 | The Customer shall be able to watermark all documents downloaded by users from the system as UNCONTROLLED at the point of download. |  |
| 7.3 | The System shall alert users if temporary revisions or additional supplements are active when downloading documents. |  |
| 7.4 | The System shall allow the customer author to select/de-select/author/edit revision highlights for each nationalisation. |  |
| 7.5 | The System shall allow the customer author to select/de-select/edit automatic revision marks for each nationalisation. |  |
| 7.6 | The System shall have the functionality for each document to have a release authorisation chain with specified users that can be easily managed and audited by an administrator. |  |
| 7.7 | The System shall store information relating to the authorisation of each nationalisation within each document that can be easily audited by an administrator. |  |
| 7.8 | The System shall allow a means of exporting a reference list of all nationalisations incorporated into a document for audit purposes (HTML, CSV, Excel, PDF). |  |
| 7.9 | The System shall have a customer defined timed review function for each nationalisation. |  |

|  |  |  |
| --- | --- | --- |
| 7.10 | The System shall notify the user of any read and sign that hasn’t been acknowledged. |  |
| **8** | **Analytics** |  |
| 8.1 | The system should provide the customer with a powerful and intuitive data analytics capability.  This Data Analytics capability will allow the customer to drill down into all available datasets and provide actionable insights that can be used to improve efficiency, safety and compliance. |  |
| 8.2 | It shall be possible to report on documents read and acknowledged. |  |
| 8.3 | It shall be possible to report on multiple metrics including but not limited to the current status of all documents in the System, document viewing numbers within adjustable time periods, individual user, device and role group usage levels and which documents have exceeded a pre-determined expiry or review date. |  |
| 8.4 | It shall be possible to create custom reports based on all metadata metrics held in the System. |  |
| 8.5 | It shall be possible to report on documents held on user devices at both the user and device level, including whether current revisions are held. |  |
| 8.6 | There shall be a full audit trail for all actions within the system, including but not limited to manual content authoring/review/approval, document downloads at both user and device level and read and sign at user level. |  |
| 8.7 | Audit trails shall be live, shall be easily accessible within the system and retained as directed by the customer. |  |
| 8.8 | The audit trail information shall be available/able to be published in multiple formats (HTML, CSV, Excel, PDF) for reporting purposes. |  |
| 8.9 | The System shall integrate with STARS Web12 API to ensure the following crew currencies: 1) Supported App version 2) All mandated docs up to date 3) All read & sign actioned. |  |
| 8.10 | The system shall allow Task authorisers13 to remotely check the read and sign status of personnel. |  |
| 8.11 | The system shall allow Task authorisers14 to remotely check the mobile device update status of personnel. |  |
| **9** | **Interoperability** |  |
| 9.1 | The System shall be compatible with the most current systems, including but not exclusive to Flight Operations Document Manager (FODM), Less Paper Cockpit New Generation (LPCNG), FlySmart+, Ops Library Browser (OLB), Ground Administration and Servicing (GAS), ODYS, Air N@V and Load Secure Batch Media (LSBM), STARS Web, iOS, Android and Windows at all times. |  |
| 9.2 | The System shall be updated to remain compatible and interoperable with the most current systems, including but not exclusive to Flight Operations Document Manager (FODM), Less Paper Cockpit New Generation (LPCNG), FlySmart+, Ops Library Browser (OLB), Ground Administration and Servicing (GAS), ODYS, Air N@V and Load Secure Batch Media (LSBM), STARS Web, iOS, Android and Windows at all times. |  |
| 9.3 | The System shall be fully accessible via ModNet at all times. |  |
| 9.4 | The System shall provide hyperlinks for each library document to allow on and off-line access from within and outside of the System and application. |  |
| 9.5 | The System shall be capable of adapting to accommodate additional aircraft types and document formats. |  |
| 9.6 | The System shall allow for documents or folders/groups to be routinely and automatically exported to a designated external area/system (HTML, etc) so that areas of the library can be mirrored in other resource depositories. |  |
| 9.7 | The supplier shall be capable of automatically importing documents from the DO, in the format provided, into the system. |  |
| 9.8 | The system will have the facility to upload large data files (up to 200Mb). |  |
| 9.9 | The supplier shall have the ability to generate a hard copy (Hard Drive) for the customer to support business continuity in the event of unexpected system outage. |  |
| **10** | **Security** |  |
| 10.1 | Where MOD personal information is held on the system it must be kept to a minimum and in accordance with DPA 2018. |  |
| 10.2 | The system must comply with HMG Functional Standard GovS007: Security, as well as MOD security requirements outlined in the relevant Defence Conditions (DefCons), Defence Standards (DefStans), and Industry Security Notices. |  |
| 10.3 | The system shall implement processes and controls to handle documents, including MOD identifiable and personal information, classified up to the Official Sensitive (OS) level. |  |
| 10.4 | The System shall be hosted on MODCloud lab iACE/ICE and comply with all associated hosting requirements. |  |
| 10.5 | The supplier must ensure that its employees hold the required security clearances and have received necessary training to understand their responsibilities in protecting MOD information. |  |
| 10.6 | The supplier must implement cybersecurity measures to safeguard MOD information and ensure that these security requirements are communicated and enforced throughout the supply chain, in compliance with DEFSTAN 05-138 and DEFCON 658. |  |
| 10.7 | If access to a MOD site is required to support the system, the supplier must only provide personnel with the relevant security clearances. The minimum clearance level for all personnel will be specified by the Authority. The supplier must provide, in advance, details of the personnel required, including their name, date of birth, or national insurance number. |  |
| 10.8 | The supplier must attend and contribute to security meetings as required by the Authority. |  |
| **11** | **Services** | |
| 11.1 | Where documents are defined as managed, the supplier shall make changes as directed by the customer. |  |
| 11.2 | Where documents are defined as structured, the supplier shall maintain the document in a structured format as required by the customer, and offering the functionality as provided the DO. |  |
| 11.3 | Where documents require structuring, the supplier shall convert a standard document into a structured format and then maintain as required by the customer. |  |

**Annex B – Support and Performance Requirements**

|  |  |  |
| --- | --- | --- |
| **Serial** | **Requirement** | **A400M ONLY** |
| **12** | **Availability** |  |
| 12.1 | The web browser, application and physical infrastructure shall be available 24hrs a day, 365 days per year. |  |
| 12.2 | Actual uptime of the service shall exceed 99.999%. |  |
| 12.3 | The MTBF for a software incident shall not be less than 60 days. |  |
| **13** | **Process** |  |
| 13.1 | The Supplier shall be conversant with processes for handling existing ADS and TID of each platform manufacturer and airline Operation Manuals (OM) and with aviation document control and compliance requirements. |  |
| 13.2 | The Supplier shall be able to evidence in-service experience of handling ADS and TID of each platform manufacturer and airline Operation Manuals (OM). |  |
| 13.3 | The supplier shall be able to evidence in-service use of their systems. |  |
| 13.4 | The Supplier shall access ADS and TID data directly from the DO. | X |
| 13.5 | The Supplier shall handle/process/manage ADS and TID data (lmport>Integrate>Author/Edit>Review>Approve>Publish).15 |  |
| 13.6 | The Supplier shall fully manage RAF Operations Manuals & Documents. (lmport>Author/Edit>Review>Approve>Publish) as structured data. |  |
| 13.7 | For tasks classified as urgent by the customer, each individual document handling task completed by the supplier, on receipt of the task from the customer, shall take no longer than 24 hrs. (lmport>Integrate>Author/Edit>Publish). |  |
| 13.8 | For tasks classified as routine by the customer, each individual document handling task completed by the supplier, on receipt of the task from the customer, shall take no longer than 48 hrs. (lmport>Integrate>Author/Edit>Publish). |  |
| 13.9 | Following the completion of TID releases the Supplier shall provide a report to the customer detailing the actions completed relevant to that release. |  |
| 13.10 | The system shall provide a task database of all tasks raised, with customer access, which details a task number, details of the task, date of task raised, customer categorization of task (routine or urgent), customer deadline for task completion, task status, estimated completion date and actual completion date. The database shall indicate where tasks have exceeded the deadline set. |  |
| **14** | **Upgrades** |  |
| 14.1 | The supplier shall inform the Authority of upgrade frequency and impact upon services. These shall be performed out of UK office hours if possible, and in liaison with customer to arrange suitable dates and times. |  |
| 14.2 | Upgrades shall be provided at no extra cost. |  |
| 14.3 | The supplier shall demonstrate innovation within the system to improve efficiency. |  |
| **15** | **Technical Support** |  |
| 15.1 | A help system shall be available within the application which allows users to raise technical queries. |  |
| 15.2 | Technical critical issue support (i.e. support for hosted hardware and software issues that prevent use of service) shall be available by phone call 24/7. |  |
| 15.3 | Operational support (i.e. support for questions on using the application and document issues) shall be available by phone call and email within UK office hours: 07:00 to 18:00 Monday to Friday. |  |
| 15.4 | Document maintenance tasks sent to the supplier shall be returned to the customer in accordance with customer instructions, without any customer rejections. |  |
| 15.5 | It shall be possible to recover the system and all data within 4hrs. |  |
| 15.6 | All the data, and all workflow statuses, must be backed up at least once every 24hrs without impact to operability/accessibility of data. |  |
| 15.7 | The supplier should have a comprehensive Business Continuity process to maintain customer operational output including in the event of denial of service. |  |
| 15.8 | All queries raised by users will be accessible, by the customer, through a Customer Service Platform provided by the supplier which includes when the query was raised, the priority level of the query, the details of the query, the status and where closed the response to the query. |  |
| 15.9 | The query answering service will be prioritized by critical, high, medium and low priority levels. |  |
| **16** | **Training** |  |
| 16.1 | Full customer administrator and ‘Train the Trainer’ user training shall be provided by the system supplier. |  |
| 16.2 | Training materials shall be provided for both administration and end users. The materials should be in MS Word & PDF format and of sufficient quality to be used by customer administrators to train end users. |  |
| 16.3 | Training materials and content shall be updated to reflect system changes. |  |
| 16.4 | Following significant system updates, customer administrator and ‘train the trainer’ training shall be provided by the system supplier. |  |
| 16.5 | All training shall be ISO 9001/2015 compliant. |  |
| **17** | **Security** |  |
| 17.1 | All personnel involved in handling data must be security cleared to SC. |  |
| 17.2 | All data released to the customer shall be assured by the provider before delivery. |  |
| 17.3 | The System code shall be scanned for vulnerabilities prior to each release. |  |
| 17.4 | The System shall be subjected to at least annual (and preferably more frequently) independent penetration tests. |  |
| 17.5 | Any vulnerabilities findings from code scanning or penetration tests shall be remediated commensurate with the identified risks. |  |
| 17.6 | The supplier will safeguard material provided by MOD and ensure that its employees are aware of their responsibilities before they receive information. There is a mutual obligation to treat in confidence all information disclosed in connection with or under the contract. DEFCON 531. |  |
| 17.7 | The supplier will implement cyber security measures to safeguard MOD information. Supplier must be compliant and ensure the compliance of their supply chain with respect to DEFSTAN 05-138 by flowing down DEFCON 658. |  |
| 17.8 | The supplier will protect official sensitive material and will flow down security requirements to their supply chain. DEFCON 660. |  |
| 17.9 | The supplier shall attend and contribute to security working groups as required by the authority. This includes but is not limited to defence lines of development, discussions, agenda items, procedural and physical processes related to the mitigation solution. |  |
| 17.10 | In the event of mitigation solutions, if the Mitigation Solution requires access to an MOD Site, the Supplier shall only supply personnel who hold the relevant security clearances. The minimum required for all personnel shall be dictated by the Authority and the Supplier shall provide:   * details of the personnel required to conduct the range of activities in this requirement; * up to date staff rosters for each site, and as a minimum include their name, contact details and rotation dates; * advance notification of personnel, and include a minimum include their name, and date of birth or national insurance number. |  |
| **18** | **Quality Management** |  |
| 18.1 | **Quality Management System:** The Contractor shall maintain an accredited Quality Management System certification to ISO 9001:2015 or suitable alternative, with the appropriate scope to deliver contract requirements, issued by a Nationally Accredited Certification Body for the duration of the contract. |  |
| **19** | **Resource Management** |  |
| 19.1 | The supplier shall deploy resource flexibly to manage unpredictable work levels whilst meeting contractual obligations |  |
| 19.2 | The Supplier shall factor in a reasonable addition to the managed structured content in existing documentation. |  |
| 19.3 | The system shall have no practical limit to the number of hosted documents that it can store. |  |

**Annex C – Project Management SOW**

**Project Management Requirements**

* 1. **PM Reqt -1 Project Management Plan (PMP)**

A PMP shall be provided detailing the following:

* + - 1. Solution Background and detailed approach to managing project.
      2. Project organisation including key role descriptions, authority levels and key personnel (inc ToR) demonstrating that the staff available is sufficient to complete the contract.
      3. Project objectives/requirements, Scope, detailing exclusions and constraints
      4. Stakeholder management plan
      5. Any critical dependencies.
      6. Risk Management plan including an initial risk register as per DefStan05-139.
      7. Master Data Assumptions List (MDAL), this shall detail all assumptions made.
      8. Communication plan including details of planned meetings.
      9. Verification, Validation and Acceptance plan.
      10. Government Furnished Plan. Detailing what GFX, if any, are required. The plan will also explain the quantity/quality of GFX required and the required dates in order to meet the schedule proposed in the project management plan. This shall include any requirement for the Authority to provide SMEs.
      11. Project Schedule showing the activities required under the contract, identifying key milestones and progress made to date. The Contractor shall state the schedule update cycle; but, as a minimum, shall be issued to the Authority for the quarterly review meetings, as part of the progress reports.
      12. Publication Management plans, details of all deliverable publications (Training, Technical, Support etc.), timing and method of agreement.

1. **PM Reqt - 2 - Integrated Test, Evaluation and Acceptance Plan**

Detailing how the Solution and training for the use of that solution by Authority SMEs shall be tested, accredited and evaluated.

1. **PM Reqt - 3 - Configuration Management Plan.**

This plan shall detail how both deliverable and project management documentation configuration shall be managed.

1. **PM Reqt - 4 - Project Security Plan (PSP).**

The PSP shall detail how and when all aspects of the security requirement shall be met in accordance with national security policy and the Security Aspects Letter in line with the Secure by Design approach and principals. This Project Security Plan shall be adhered to throughout the term of the Contract. Any proposed changes to the security management processes undertaken at the facility shall be subject to Authority agreement during the term of the Contract.

1. **PM Reqt - 5 - Support Management Plan (SMP)**

The SMP shall clearly identify the roles and responsibilities of the Authority and Contractor and provide guidance and instruction to personnel as to how In-Service Support (ISS) will be conducted. The SMP shall also consider, but not necessarily be limited to, the following essential information:

1. Introduction.
   * 1. Overview. This section shall provide an overview of the support solution;
     2. Contractor information. This section shall identify the Contractor and relevant contact details;
     3. Abbreviations;
     4. References;
     5. Definitions. A list of definitions of the terms used throughout the document.
2. General Information.
3. Purpose. This section shall describe the purpose of the Management Plan;
4. Sub-Contractors. This section shall identify all the relevant Sub-Contractors that are utilised in the delivery of the In-Service Support and shall detail their involvement;
5. Information Systems. This section shall identify the information systems to be used for control, management and tracking of the service;
6. Product Non-Conformance. This section shall demonstrate how non-conformance shall be identified and managed.
7. Local Procedures. This section shall detail any local procedures that the Authority shall implement to assist the Contractor in the delivery of the In-Service Support.
8. Technical Support.
   1. Support for Technical Issues. This section shall detail the support available for technical issues
   2. Support for Supply Issues. This section shall detail the support available for supply issues
9. Post Design Services (PDS). This section shall;
   1. detail all procedures/processes for how PDS will be delivered, clearly articulating how Master Documentation, including Master Equipment Document Sets, will be maintained and how they will be stored to meet the requirements of the Statement of Requirements(SOR). This section shall identify storage locations/backups, as well as how the Authority can access the latest Master Documentation.
   2. also refer to the Configuration Management Plan as appropriate to demonstrate how configuration control of the Master Documentation will be implemented.
   3. The Contractor approach to the following ILS disciplines shall be summarised and referenced to detailed plans where required (and applicable) by the SOR and listed in the Contracted Deliverable Document List (CDDL). Where a discipline is considered to be non-relevant, the statement “NON- RELEVANT” shall be documented with a summary explanation. The ILS disciplines for this project are:
   * Support Assurance;
   * ISS Performance Monitoring;
   * Configuration Management;
   * Obsolescence Management;
   * Supply Support;
   * Packaging Handling Storage & Transportation (PHS&T);
   * Disposal;
   * Technical Information Management;
   * Support and Test Equipment (S&TE);
   * Human Factors Integration (HFI);
   * Supportability Analysis (SA);
   * Availability Reliability and Maintainability (AR&M);
10. **PM Reqt - 6 - Training Plan**

The training plan shall include the development of the training solution, the proposed process for agreeing and documenting the training solution with the User. Deliver the training to the agreed schedule and formally deliver the course material to the Authority.

1. **PM Reqt - 7 - Meetings**

Unless agreed to the contrary, the Contractor is to facilitate progress meetings at the locations shown against each meeting in accordance with DEFCON 642.

The following meetings are to be held as a minimum:

* + - 1. Inaugural meeting within 2 weeks of contract award - Contractors premises or via TEAMS.
      2. Quarterly Progress meetings – MOD facility/Contractors premises or via TEAMS.
      3. Reviews, implementation discussions and other meetings required to fulfil the contract – MoD facility/contractor premises or via TEAMS.

1. **PM Reqt - 8 - Agenda and Progress reports**

The Contractor is to provide an agenda, and a progress report prior to all quarterly meetings in accordance with DEFCON 604, 2 weeks prior to all meetings, which is to include as a minimum:

* + - 1. Progress made to date.
      2. Project Management and Timescales Issues.
      3. Risk management activities and review of Risks and Issues arising (Including early identification of risks and issues).
      4. Validation and Acceptance.
      5. Forward plan.
      6. Quality.
      7. Security.
      8. Finance and Commercial.

Draft minutes for all meetings are to be provided to the Authority Project Manager within 2 weeks of the date of meeting and issued within one week of the minutes being agreed with the Authority Project Manager.

1. **PM Reqt – 9 – Safety Management**

The Contractor is to comply with Def Stan 00-56 – Part 1 Issue 8 to (latest amendment or issue) and relevant and current UK and EU legislation including but not limited to ISO 9001, and the Health and Safety (H&S) at work act. All safety related materials including documentation, plans, certificates etc. shall be made available upon request for independent audit.

1. **PM Reqt – 10- Quality Management**

No Deliverable Quality Plan is required but the Contractor shall make a firm commitment to maintain its Quality Management System in accordance with the applicable standards. The Authority is fully committed to ISO 9001:2015 and the Contractor shall be registered to this Standard to meet the Quality Management requirements of Ministry Contracts. For the purposes of the Contract, the following Quality Assurance Standards shall apply:

* + - 1. AQAP 2110 Edition D Version 1 NATO Quality Assurance Requirements for Design, Development and Production.
      2. Certificates of Conformity (CoC) shall be provided in accordance with DEFCON 627
      3. AQAP 2210 Edition A Version 2 - NATO Supplementary Software Quality Assurance Requirements to AQAP 2110 or AQAP 2310 shall apply.
      4. Any Contractor working parties shall be provided in accordance with DEFSTAN 05-61 Part 4, Issue 4 – Quality Assurance Procedural Requirements – Contractor Working Parties
      5. For guidance on the application and interpretation of AQAPs refer to the appropriate AQAP Standards Related Document (SRD).
      6. Where Government Quality Assurance (GQA) is performed against this contract it will be in accordance with AQAP 2070 Edition B Version 4.

1. **PM Reqt – 11 – Risk Management**

The Authority requires quarterly review meetings to review and agree the ownership of any risks which could affect the contractual requirements, which will be based on the principle that the organisation best able to manage a risk will accept ownership of the risk. Early identification of risks and issues affecting the Contract will ensure prompt action to mitigate and resolve risks before they have an impact on capability.

The Authority requires a Risk & Opportunity Management Plan (ROMP) that documents the Contractor’s plan for managing risks. The Plan must contain, but is not necessarily limited to, the following essential information:

* + - 1. The process by which the identification, analysis and planning of risks will be undertaken and managed.
      2. Organisation roles and responsibilities, including:
    1. Identification of risk management organisation for the Project, including contact details;
    2. Identification of specific roles;
    3. Terms of Reference for individuals involved in risk management;
    4. Risk Management Training and competency.
       1. Methodology for Risk Management, including:

The contractor shall explain how the risk management method relates to other project control methods i.e. The relationship between risk management and the project schedule;

The scoring and interpretation methods appropriate for the type and timing of the qualitative and quantitative risk analysis being performed.

* + - 1. Risk Management Activities; including:

How the risk management method will be applied throughout any sub-contractor hierarchy;

Risk escalation, including the Contractor’s internal process for escalation and escalation from Contractor to The Authority;

Stakeholder Management, including the interaction with the Project Team.

* + - 1. Reviews and reporting procedures, including:
    1. Frequency of audit and review of the project risk management process;
    2. Review meeting structure, including the Terms of Reference for the Review Meeting;
    3. Frequency of risk review meetings;
    4. Risk review reporting format to be produced for these meetings to demonstrate the management of mitigation actions and progress in reducing/eliminating risks;
    5. Discussion of risk priority ranking and further actions;
    6. Support to Authority risk reviews;
    7. A proposed procedure to update and maintain Contractor owned risk information in the Authority’s Risk & Opportunity Register.
       1. Document the Tools and Techniques that will be utilised to identify, assess and manage risks.
       2. Risk Terminology/Definitions, to ensure common understanding between The Authority & Contractor.
       3. The Authority requires a Risk & Opportunity Register to document the Contractor’s project risks and relevant mitigations. The register must contain, but is not necessarily limited to, the following essential information:

i. Identifier: A unique serial number for each risk entry;

1. Identification Date: The date that the risk was first identified;
2. Risk/Opportunity Owner: The nominated individual who is accountable for the management of the risk. (The owner must possess the requisite authority for the task, particularly in addressing the cause of a risk);
3. Risk/Opportunity Category: A grouping based on either the cause or consequence of a risk event. (For example, resource, people, equipment etc.);
4. Risk/Opportunity Cause: A comprehensive narrative description of the risk cause;
5. Risk/Opportunity Event: A comprehensive narrative description of the risk event;
6. Impact Description: A narrative description of the impact (degree of) the risk will have on the Project if it was to occur;
7. Probability Assessments: An estimate as a percentage of the likelihood of the risk occurring (as detailed in Table 1). For each risk entry the recording of separate pre- and post- mitigation assessments is required;
8. Impact Assessments: An estimate of the impact on the Project should the risk/opportunity occur. Estimated against time, cost and performance (as detailed in Table 1). For each risk entry the recording of a separate pre- and post- mitigation assessments is required;
9. Combined Assessments: A combined score (Probability x Impact) on a scale of 1-25 (as detailed in Table 2). For each risk/opportunity entry the recording of separate pre- and post- mitigation assessments is required;
10. Mitigation Actions: Specific actions or controls to be implemented to reduce the probability and/or impact of the risk,or enhance/exploit potential opportunities. To include consideration of Cost Benefit Analysis;
11. Mitigation Target Dates: The expected completion date for each identified mitigation action;
12. Mitigation Action Owner: The nominated individual who will be responsible for the implementation of action(s) to mitigate the risk or enhance/exploit the opportunity. (Owners should be the person best placed to optimise delivery of the task);
13. Fall-back Plan: What action will be undertaken (to include start and finish dates where applicable), to minimise the impact of a risk following its realisation;
14. Review Date: The date that the risk and mitigation actions were last reviewed.

i. A Risk Management software tool may be used but is not mandated (the Authority is familiar with the ‘Active Risk Manager’ (‘ARM’).

j. Demonstration of an initial risk identification and population of the register with specific risks to the fulfilment of the contract is mandated at the Tender stage. Post contract award the actual level of impact within the Contract will be agreed upon discussion between the Supplier and Authority and will depend upon Contract details.

k. Post contract award the Risk & Opportunity Register is to be reviewed and maintained in accordance with the Risk Management Plan.

