Schedule of Requirements – Ministry of Defence Standardised Contracting Template 2 (SC2) containing:

ITEM 1
SC2 Standard Contract Conditions
ITEM 2
Schedule 1 – Definitions

Schedule 2 - Statement of Requirement
Annex A to Schedule 2 – Pricing of the Statement of Requirements
Annex B to Schedule 2 – Authority Dependencies
Annex C to Schedule 2 – Contractor Key Roles
Annex D to Schedule 2 – Contractor Assumptions
Annex E to Schedule 2 – Contractor Exclusions
Schedule 3 - Contract Data Sheet for Contract No: CCDT/491

Schedule 4 - DEFFORM 111 – Appendix to Contract - Addresses and Other Information

Schedule 5 - Tenderer's Commercially Sensitive Information Form (DEFFORM 539A)

Schedules 6 & 7 - not used

Schedule 8 – Implementation Plan
Annex A to Schedule 8 - Data Migration Plan
Annex B to Schedule 8 – Software Configuration Plan
Annex C to Schedule 8 – Software and Network Approval Plan
Appendix A to Schedule 8 – MoSCoW Definition to be used in a Fall Back scenario

Schedule 9 – Training Plan

Schedule 10 – Exit Strategy
Annex A to Schedule 10 – Exit Plan

Schedule 11 – Service Levels, Service Level Agreements and Service Credits
Annex A.1 to Schedule 11 – Technical Support
Annex A.2 to Schedule 11 - Service Level Agreement
Appendix A to Annex A.2 to Schedule 11 – Service Level Agreement - Metrics
Annex B to Schedule 11 – System Administration Service Level Agreement

Schedule 12 – Business Continuity and Disaster Recovery
Annex A to Schedule 12 – Business Continuity and Disaster Recovery Plan

Schedule 13 – Additional Tasking Process
Annex A to Schedule 13 - Tasking Order Form to CCDT/491
Annex B to Schedule 13 – Rate Card for Additional Services
Annex C to Schedule 13 – Additional Skill Levels Defined

Schedule 14 – Not Used

Schedule 15 – User Access Control

Schedule 16 – Security Aspects Letter

Schedule 1 - Definitions of Contract

Articles	means the Contractor Deliverables (goods and/or the services), including Packaging (and Certificate(s) of Conformity and supplied in accordance with any QA requirements if specified) which the Contractor is required to provide under the Contract in accordance with Schedule 2 (Schedule of Requirements), but excluding incidentals outside Schedule 2 (Schedule of Requirements) such as progress reports. (**This definition only applies when DEFCONs are added to these Conditions**);
Authority	means the Secretary of State for Defence acting on behalf of the Crown;
Authority's Representative(s)	shall be those person(s) defined in Schedule 3 (Contract Data Sheet) who will act as the Authority's Representative(s) in connection with the Contract. Where the term "Authority's Representative(s)" in the Conditions is immediately followed by a functional description in brackets, the appropriate Authority's Representative(s) shall be the designated person(s) for the purposes of condition 8;
Business Day	means 09:00 to 17:00 Monday to Friday, excluding public and statutory holidays;
Central Government Body	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a. Government Department; b. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c. Non-Ministerial Department; or d. Executive Agency;
Collect	means pick up the Contractor Deliverables from the Consignor. This shall include loading, and any other specific arrangements, agreed in accordance with clause 28.c and Collected and Collection shall be construed accordingly;
Commercial Packaging	means commercial Packaging for military use as described in Def Stan 81-041 (Part 1)
Conditions	means the terms and conditions set out in this document;
Consignee	means that part of the Authority identified in Schedule 3 (Contract Data Sheet) to whom the Contractor Deliverables are to be Delivered or on whose behalf they are to be Collected at the address specified in Schedule 3 (Contract Data Sheet) or such other part of the Authority as may be instructed by the Authority by means of a Diversion Order;
Consignor	means the name and address specified in Schedule 3 (Contract Data Sheet) from whom the Contractor Deliverables will be dispatched or Collected;
Contract	means the Contract including its Schedules and any amendments agreed by the Parties in accordance with condition 6 (Amendments to Contract);
Contract Price	means the amount set out in Schedule 2 (Schedule of

	Requirements) to be paid (inclusive of Packaging and exclusive of any applicable VAT) by the Authority to the Contractor, for the full and proper performance by the Contractor of its obligations under the Contract.
Contractor	means the person who, by the Contract, undertakes to supply the Contractor Deliverables, for the Authority as is provided by the Contract. Where the Contractor is an individual or a partnership, the expression shall include the personal representatives of the individual or of the partners, as the case may be, and the expression shall also include any person to whom the benefit of the Contract may be assigned by the Contractor with the consent of the Authority;
Contractor Commercially Sensitive Information	means the Information listed in the completed Schedule 5 (Contractor's Commercially Sensitive Information Form), which is Information notified by the Contractor to the Authority, which is acknowledged by the Authority as being commercially sensitive;
Contractor Deliverables	means the goods and/or the services, including Packaging (and Certificate(s) of Conformity and supplied in accordance with any QA requirements if specified) which the Contractor is required to provide under the Contract as per Schedule 2;
Control	means the power of a person to secure that the affairs of the Contractor are conducted in accordance with the wishes of that person: a. by means of the holding of shares, or the possession of voting powers in, or in relation to, the Contractor; or b. by virtue of any powers conferred by the constitutional or corporate documents, or any other document, regulating the Contractor; and a change of Control occurs if a person who Controls the Contractor ceases to do so or if another person acquires Control of the Contractor;
CPET	means the UK Government's Central Point of Expertise on Timber, which provides a free telephone helpline and website to support implementation of the UK Government timber procurement policy
Crown Use	in relation to a patent means the doing of anything by virtue of Sections 55 to 57 of the Patents Act 1977 which otherwise would be an infringement of the patent and in relation to a Registered Design has the meaning given in paragraph 2A(6) of the First Schedule to the Registered Designs Act 1949;
Dangerous Goods	means those substances, preparations and articles that are capable of posing a risk to health, safety, property or the environment which are prohibited by regulation, or classified and authorised only under the conditions prescribed by the: a. Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009 (CDG) (as amended 2011); b. European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR); c. Regulations Concerning the International Carriage of Dangerous Goods by Rail (RID); d. International Maritime Dangerous Goods (IMDG) Code; e. International Civil Aviation Organisation (ICAO) Technical Instructions for the Safe Transport of Dangerous Goods by Air; f. International Air Transport Association (IATA) Dangerous Goods Regulations.

DBS Finance	means Defence Business Services Finance, at the address stated in Schedule 3 (Contract Data Sheet);
DEFCON	means the MOD DEFCON series which can be found at https://www.aof.mod.uk**;**
DEFFORM	means the MOD DEFFORM series which can be found at https://www.aof.mod.uk;
DEF STAN	means Defence Standards which can be accessed at https://www.dstan.mod.uk;
Deliver	means hand over the Contractor Deliverables to the Consignee. This shall include unloading, and any other specific arrangements, agreed in accordance with condition 28 and Delivered and Delivery shall be construed accordingly;
Delivery Date	means the date as specified in Schedule 2 (Schedule of Requirements) on which the Contractor Deliverables or milestones or the relevant portion of them are to be Delivered or made available for Collection;
Denomination of Quantity (D of Q)	means the quantity or measure by which an item of material is managed;
Design Right(s)	has the meaning ascribed to it by Section 213 of the Copyright, Designs and Patents Act 1988;
Diversion Order	means the Authority's written instruction (typically given by MOD Form 199) for urgent Delivery of specified quantities of Contractor Deliverables to a Consignee other than the Consignee stated in Schedule 3 (Contract Data Sheet);
Effective Date of Contract	means the date specified on the Authority's acceptance letter;
Evidence	means either: a. an invoice or delivery note from the timber supplier or Subcontractor to the Contractor specifying that the product supplied to the Authority is FSC or PEFC certified; or b. other robust Evidence of sustainability or FLEGT licensed origin, as advised by CPET;
Firm Price	means a price (excluding VAT) which is not subject to variation;
FLEGT	means the Forest Law Enforcement, Governance and Trade initiative by the European Union to use the power of timber-consuming countries to reduce the extent of illegal logging;
Go-Live Date	24 June 2019
Government Furnished Assets (GFA)	is a generic term for any MOD asset such as equipment, information or resources issued or made available to the Contractor in connection with the Contract by or on behalf of the Authority;
Hazardous Contractor Deliverable	means a Contractor Deliverable or a component of a Contractor Deliverable that is itself a hazardous material or substance or that may in the course of its use, maintenance, disposal, or in the event of an accident, release one or more hazardous materials or substances and each material or substance that may be so

released;

Independent Verification	means that an evaluation is undertaken and reported by an individual or body whose organisation, systems and procedures conform to "ISO Guide 65:1996 (EN 45011:1998) General requirements for bodies operating product certification systems or equivalent", and who is accredited to audit against forest management standards by a body whose organisation, systems and procedures conform to "ISO 17011: 2004 General Requirements for Providing Assessment and Accreditation of Conformity Assessment Bodies or equivalent";
Information	means any Information in any written or other tangible form disclosed to one Party by or on behalf of the other Party under or in connection with the Contract;
Issued Property	means any item of Government Furnished Assets (GFA), including any materiel issued or otherwise furnished to the Contractor in connection with the Contract by or on behalf of the Authority;
Legal and Sustainable	means production and process methods, also referred to as timber production standards, as defined by the document titled "UK Government Timber Production Policy: Definition of legal and sustainable for timber procurement". The edition current on the day the Contract documents are issued by the Authority shall apply;
Legislation	means in relation to the United Kingdom any Act of Parliament, any subordinate legislation within the meaning of section 21 of the Interpretation Act 1978, any exercise of Royal Prerogative or any enforceable community right within the meaning of Section 2 of the European Communities Act 1972;
Military Level Packaging (MLP)	means Packaging that provides enhanced protection in accordance with Def Stan 81-041 (Part 1), beyond that which Commercial Packaging normally provides for the military supply chain;
Military Packager Approval Scheme (MPAS)	is a MOD sponsored scheme to certify military Packaging designers and register organisations, as capable of producing acceptable Services Packaging Instruction Sheet (SPIS) designs in accordance with Defence Standard (Def Stan) 81-041 (Part 4);
Military Packaging Level (MPL)	shall have the meaning described in Def Stan 81-041 (Part 1);
MPAS Registered Organisation	is a packaging organisation having one or more MPAS Certificated Designers capable of Military Level designs. A company capable of both Military Level and commercial Packaging designs including MOD labelling requirements;
MPAS Certificated Designer	shall mean an experienced Packaging designer trained and certified to MPAS requirements;
NATO	means the North Atlantic Treaty Organisation which is an inter-governmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949;
Notices	shall mean all Notices, orders, or other forms of communication required to be given in writing under or in connection with the Contract;

Overseas	shall mean non- UK or foreign;
Packaging	Verb. The operations involved in the preparation of materiel for; transportation, handling, storage and Delivery to the user; Noun. The materials and components used for the preparation of the Contractor Deliverables for transportation and storage in accordance with the Contract;
Packaging Design Authority (PDA)	shall mean the organisation that is responsible for the original design of the Packaging except where transferred by agreement. The PDA shall be identified in the Contract, see Annex A to Schedule 3 (Appendix – Addresses and Other Information), Box 3;
Parties	means the Contractor and the Authority, and Party shall be construed accordingly;
Primary Packaging Quantity (PPQ)	means the quantity of an item of material to be contained in an individual package, which has been selected as being the most suitable for issue(s) to the ultimate user, as described in Def Stan 81-041 (Part 1);
Recycled Timber	means recovered wood that prior to being supplied to the Authority had an end use as a standalone object or as part of a structure. Recycled Timber covers: a. pre-consumer reclaimed wood and wood fibre and industrial by-products; b. post-consumer reclaimed wood and wood fibre, and driftwood; c. reclaimed timber abandoned or confiscated at least ten years previously; it excludes sawmill co-products;
Resolve or RESOLVE	means an off-the Shelf Airworthiness Issues Management System provided by the Contractor to meet the DES AIMS requirement as per Schedule 2.
Safety Data Sheet	has the meaning as defined in the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulations 2007 (as amended);
Schedule of Requirements	means Schedule 2 (Schedule of Requirements), which identifies, either directly or by reference, Contractor Deliverables to be provided, the quantities and dates involved and the price or pricing terms in relation to each Contractor Deliverable;
Short-Rotation Coppice	means a specific management regime whereby the poles of trees are cut every one to two years and which is aimed at producing biomass for energy. It is exempt from the UK Government timber procurement policy. For avoidance of doubt, Short-Rotation Coppice is not conventional coppice, which is subject to the timber policy;
Specification	means the description of the Contractor Deliverables, including any specifications, drawings, samples and / or patterns, referred to in Schedule 2 (Schedule of Requirements);
STANAG 4329	means the publication NATO Standard Bar Code Symbologies which can be sourced at https://www.dstan.mod.uk/faqs.html;
Subcontractor	means any subcontractor engaged by the Contractor or by any other subcontractor of the Contractor at any level of subcontracting

to provide Contractor Deliverables wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract and 'Subcontract' shall be interpreted accordingly;

Timber and Wood-Derived Products means timber (including Recycled Timber and Virgin Timber but excluding Short-Rotation Coppice) and any products that contain wood or wood fibre derived from those timbers. Such products range from solid wood to those where the manufacturing processes obscure the wood element;

Transparency Information means the content of this Contract in its entirety, including from time to time agreed changes to the Contract, and details of any payments made by the Authority to the Contractor under the Contract;

Schedule 2 - The Schedule of Requirement

1 Definitions

1.1 In this Schedule 2 the following definitions shall apply:

Action	means an activity (including authorisations against decisions) assigned to a User as part of the execution of a Process whilst responding to an Event or managing an Issue.
Air Safety	is the state of freedom from unacceptable risk of injury to persons, or damage, throughout the life cycle of military Air Systems. Its purview extends across all Defence Lines of Development and includes Airworthiness, Flight Safety, policy, regulation and the apportionment of resources. It does not address survivability in a hostile environment.
Air System	means a fixed or rotary wing aircraft, piloted or remotely piloted, and the ground-based systems vital to their safe operation.
Air System Document Set (ADS)	means the documentation considered as essential for sustaining the Type Airworthiness and maintaining the continuing Airworthiness, and for ensuring the safe operation of an Air System. The documentation is defined, maintained and approved for use by the Type Airworthiness Authority.
Airworthiness	means the ability of an Air System or other airborne equipment or system to be operated in flight and on the ground without significant hazard to aircrew, ground crew, passengers or to third parties; it is a technical attribute of materiel throughout its lifecycle.
Airworthiness Issues	means equipment faults/failings that may impact airworthiness, air-safety, availability and/or operating capability of air systems/equipment. Airworthiness Issues can be reported from a range of sources: Front Line Commands; Design Organisations; DE&S; and other operating nations (through a DE&S interface). They are often interdependent, linked or could be merged into one another. Appropriate actions to investigate and respond to many of them are strictly governed by Military Aviation Authority (MAA) Regulations.
Artefacts	means discrete data items (i.e an airworthiness related document that can be used as evidence in making an airworthiness judgement) attached to an Issue or Entity to form part of the evidence trail.
Authorised User(s)	means any person having been given access to the DES AIMS by the Authority. This will include, but is not limited to, people within DE&S, Front Line Commands, Design Organisations and industry partners.
Authority to Operate (AtO)	means the risks or issues introduced by the service are accepted and the service has proven it can meet the Users needs. The service is authorised to operate within its agreed parameters. Only when the service deviates beyond these parameters will it be required to revisit the release process. An AtO is given to projects following a successful probationary period after the introduction or change to an ICT Service. It is issued by the Network Operating Authority following its

	assessment of behavior of the Service.
Authority to Test (AtT)	means the authority to release the service tied to the scope requested within the technical release readiness assessment and associated test plans. At this stage authority will be granted if the risks are deemed acceptable against the scope of testing, there maybe risks that are not necessarily acceptable for IAtO.
Authority Zone	Authority Zones focus on the level of security governance and document control officer coverage that the MoD is able to exercise over services. This reflects the freedom of action which the MoD has over such services and the ability the MoD has to directly respond to threats to the MoD's ICT based information assets.
CoMPI	CoM (Chief of Materiel) Air Policy Instructions are DE&S internal policies used to govern activities within the air environment.
Critical Acceptance Criteria	means Pre-established standards or requirements a product or project must meet.
DART	means the Defence Assurance Risk tool which is used to enable anyone with an account to initiate, input to and track various information assurance related requirements
Data Room	means the electronic depository hosted on the AWARD tool and designated as the 'electronic data room' by the Authority in which information will be stored.
Defence Lines of Development (DLOD)	means a useful summary of the range of factors that need to be considered when making decisions on capability and force structure including training, equipment, personnel, information, doctrine and concepts, organisation, infrastructure and logistics.
Defence Cyber Operations (DCO)	means the measures in place to identify and manage cyber risk and the passive and active means to project in and from cyberspace.
DE&S Airworthiness Issue Management System (DES AIMS)	means the off-the shelf software package being procured by DE&S to meet their software requirement for an off the shelf Airworthiness Issues Management System in accordance with the requirement Part A below that enables all Airworthiness Issues to be identified, reported and managed. Management of Airworthiness Issues is the undertaking of processes, tasks and actions to resolve them, and the ability to monitor progress of the Airworthiness Issue.
Design Organisations	Means the approved organisation responsible for the overall design or through-life configuration management of the design of each product, part or appliance installed in an Air System.
DNS	The Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
Duty Holder (DH)	means the individual legally accountable for the safe operation of Air Systems in their AoR and for ensuring that risks to life are as low as reasonably practicable and tolerable. DH have a personal level duty of care for the personnel under their command; those who, by virtue of their temporary involvement in aviation activities, come within an DH's Area of Responsibility (AoR); and the wider public who may be affected by their operations.
DH's Area of Responsibility (AoR)	Means the Air Systems (and related teams, personnel and processes) a Duty Holder is responsible for.
Entity(ies)	means the artefacts and data produced as an outcome of executing Processes end to end. Creating a record of all Actions and decisions made throughout a Process to assist in the management of an Issue or Event.
Event	means any unforeseen in-service arising relating to an Air System that someone believes might compromise airworthiness and therefore requires the attention of the Type Airworthiness Authority. These events come from a number of sources in multiple formats. Events may be escalated to an Issue or linked to existing issues.
Export	means the ability to create a data file that can be utilised outside of the

	DES AIMS to provide input (in accordance with defined data dictionary entries) into another key air environment tools (either MoD or Industry owned), provide an output of data in support of other MoD processes (air investigations for example), provide output in support of DE&S corporate dashboards or to provide full output of the AIMS for the purposes of transition to another future AIMS tool.
Flight Safety	means a collective endeavour to operate in the air environment safely, it embraces any activity that contributes to the safe operation of military airworthy systems in flight or on the ground.
Front Line Command (FLC)	The single-Service Commands (Navy, Land or Air) responsible for operating, administering or training its forces outside the requirements of joint operations.
Interim Authority to Operate (IAtO)	Means the approval given by ISS where the risks or issues introduced by the service are known and deemed to be acceptable to allow the system to connect to the network for a probationary period of up to 6 months, to test and verify in the live environment, prior to full AtO being granted.
ISS	means the Information Systems and Services organisation within the UK MoD whose responsibility is information and communications technology support for MoD operations and business
Issue	is a means for capturing, escalating, investigating and resolving events (singular or multiple linked together) that could compromise the airworthiness of the Air System. An Issue allows an easily accessible audit trail of activities, actions and decisions aimed at mitigating risk to an Air System.
Manual of Maintenance and Airworthiness process (MAP)	The Manual of Maintenance and Airworthiness Process (MAP-01) supports the 4000 series of MAA processes which regulate continuing airworthiness engineering activity to sustain military in service aircraft.
Military Aviation Authority (MAA)	The Military Aviation Authority is an independent organisation responsible for regulating Air Safety across defence. MAA is part of the Ministry of Defence.
Military Continuing Airworthiness Management Organisation (Mil CAMO)	develops and controls the Aircraft Maintenance Programme iaw the Air System Document Set (ADS) endorsed by the TAA.
MRP	MAA Regulatory Publications
Network Operating Authority (NOA)	The Network Operating Authority (NOA) provides day-to-day operational management of the Defence network, monitoring and managing more than 750,000 configurable IT assets. Network Operating Authority: protects, operates and defends the Defence network thereby preserving its operational capability and integrity.
Privacy Impact Assessment (PIA)	means the process that enables organisations to anticipate, identify and address the potential privacy impacts of new initiatives or systems on individuals privacy. The identified risks to an individual's privacy can be managed through consultation with key stakeholders and where applicable systems can be designed to avoid unnecessary privacy intrusion.
Process(es)	means the execution of various workflows with associated tasks or Actions with the aim of providing a resolution to any event or issue (processes and workflows are defined in Annex A)
Recovery Point Objective (RPO)	means the maximum targeted period in which data might be lost from an IT service due to a major incident.
Recovery Time Objective (RTO)	means the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
RMADS	means the Risk Management and Accreditation Document Set that sets out the system, the identified risks, the security controls applied and lists all the applicable documents to accreditation, risk and other through life management activities. This is reviewed by the accreditor

	and subsequently approved.
Service Level Agreement (SLA)	means a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider.
Type Airworthiness Authority (TAA)	means the individual who on behalf of the Secretary of State, oversees the airworthiness of specified Air System types.
User	means Authorised User

2 Introduction

2.1 This Annex sets out Defence Equipment and Supports' requirement for the provision of an 'off the shelf' Airworthiness Issues Management System (AIMS) that enables all Airworthiness Issues to be identified, reported and managed. The management of Airworthiness Issues is undertaken through a set of processes', tasks and actions and includes the ability to monitor progress of the Airworthiness Issue as well as providing an audit trail of actions taken. The resolution of Airworthiness Issues is key to maintaining the design airworthiness of the Air Systems and equipment for the duration of their operational lives. Although responsibility for the resolution of Airworthiness Issues sits with a DE&S delivery team's Type Airworthiness Authority (TAA), it is also reliant on specialists who reside outside DE&S within civilian industry, such as Design Organisations and Front Line Command organisations.

3 The Requirement

3.1 The DES AIMS requirement is for:

- Part A – The DES AIMS software requirement (provided for information as off-the shelf Software confirmed as meeting the requirement during the ITT process);
- Part B – The DES AIMS implementation requirement;
- Part C – The DES AIMS service requirement.

3.2 Each of these Parts of the DES AIMS is described in the tables below.

Part A – The DES AIMS software requirement

Serial	Requirement
A.1 - Key Software functionality	
1	The DES AIMS software shall enable the reporting and management of Airworthiness Issues by Authorised Users.
2	The management of Airworthiness Issues is complex due to interdependencies and wide-span of stakeholders and provides essential support to operational Air Systems and associated equipment. The DES AIMS software must be able to manage high volumes of complex Airworthiness Issues.
3	The DES AIMS software shall support 6,300 Authorised Users with an appropriate concurrency of use to meet the DES AIMS Part B and C requirement.
4	The DES AIMS software shall facilitate the management of Airworthiness Issues by enabling the undertaking of tasks, decisions and Actions to lead to the resolution of Airworthiness Issues, including linked Processes, as required.
5	The DES AIMS software shall provide a full and comprehensive chronological audit trail of decisions and evidence underpinning Issues and Entities
6	The DES AIMS software shall provide the ability to generate a snapshot of all data related to a single Air System, without disrupting day-to-day business, within 1 hour of any given moment. This snapshot shall be an un-editable baseline of the data set in order to deliver credible data to the Defence Air Accident Investigation Board in the event of an accident.
7	The supplier shall ensure that all data (including archived material) is accessible 24/7 365 days per year to all Authorised Users
8	The DES AIMS software shall be based on one consistent logical database structure, including consistent naming conventions and table / entity structures.
9	The DES AIMS software shall provide an audit trail of all Authorised User activity within the system
10	The DES AIMS software shall enable data to be interfaced / exchanged with other MoD and Industry owned airworthiness and business software tools.
11	The DES AIMS software shall provide the ability to flexibly configure Authorised User access controls and permissions as per the Access Strategy in the Data Room.
A.2 – Compliance with workflows	
1	The DES AIMS software shall enable compliance with: - MAA Regulations; - Air Environment policy; and - Internal DE&S procedures; The reporting and management of Airworthiness Issues for DE&S is broken down into 41 workflows with details for each of the extant workflows showing the steps involved and required forms / fields (see AIMS Process Requirements in the Data Room). References to MAA Regulations (e.g RA1410) are provided as hyperlinks within the individual workflows within the AIMS Process Requirements in the Data Room. The workflows are grouped by the reporting and management areas they support as follows:
2	- **MAA regulations**: - Narrative fault (MF760) reporting raised and delivered for military owned Air Systems in line with MAP-01, Chapter 7.5.1 and CoMPI 16 ; - Air System Document Set (ADS) Unsatisfactory Feature Report (UFR) (MF765) raised and delivered for military owned Air Systems in line with MAP-01, Chapter 8.2.1 and CoMPI 14; - ADS UFR (MF765x) raised and delivered for military owned Air Systems in line with MAP-01, Chapter 8.2.1 and CoMPI 14; - Occurrence reporting via Defence Air Safety Occurrence Reports (DASORs) raised and delivered iaw RA1410 - Occurrence reporting via Significant Engineering Safety Occurrence Reports (SESORs) raised and delivered iaw RA1410 - Special instructions (technical) (iaw MAP-01, Chapter 10.5.3) - Service modification (iaw RA5308) - Quality occurrence reports (QORs) raised and delivered iaw MAP-01, Chapter 15.1.1. - Design organisation modifications (iaw RA5313 – Design Modifications) - Air system topic 2 (N/A/R)1 (iaw RA4356 - Topic 2(N/A/R)1 MAP-01 Chap 8.4)

3	- **Air environment policy**:
	  - Issues (no MRP requirements);
	  - Safety assessment (no MRP requirements);
	  - Management of equipment hazards (iaw RA1210);
	  - Technical enquiries (no MRP requirements)
	  - Aircraft integrity management data (iaw RA5720)
	  - Service inquiry recommendations (iaw RA1410)
	  - Supplier concessions - part of configuration management (iaw RA5311)
	  - General messaging (no MRP requirements)
	  - Leaflet 103E management (no MRP requirements)
	  - Leaflet 109d management (no MRP requirements)
	  - Signal amendment (no MRP requirements)
	  - Support policy letters (no MRP requirements)
	  - Engineering concessions (no MRP requirements)
	  - Service bulletins (no MRP requirements)
	  - Reportable occurrences (no MRP requirements)
	  - Technical publication request form (raised and delivered for military owned Air Systems in line with MAP-01, Chapter 8.2.1)
	  - Design Organisation repairs 2 (N/A/R)5 (iaw RA5865 – Design Repairs)
	  - Technical Warnings (no MRP requirements)
	  - Special flying instructions (no MRP requirements)
	  - Operational occurrence reports (no MRP requirements)
	  - Special technical orders (investigation) (no MRP requirements)
	  - Special technical orders (change) (no MRP requirements)
	  - Data change requests (no MRP requirements)
	  - Upload mass properties (no MRP requirements)
	  - Engineering support demands (no MRP requirements)

4	- **Internal DE&S procedures**:
	  - Management activity (no MRP requirements)
	  - Production System Configuration (PSC) lookup table (service modification enabler) (no MRP requirements)
	  - Extension requests (lifting and maintenance) (no MRP requirements)
	  - Deviation reports (no MRP requirements)
	  - Aircraft structural health monitoring (no MRP requirements)
	  - Structural zonal inspections (Topic 5V) (no MRP requirements)

A.3 – Software functionality	

1	The DES AIMS software shall enable Authorised Users to:
	- Access the tool via a web front end from a variety of browser types;
	- Originate, process, track and record Issues and / or Entities;
	- Record details of record, retain and recover details of all Events;
	- Assign and reassign Issues and / or Entities to another User;
	- Assign Actions to other Users with User defined timelines, deadlines and priorities;
	- Complete mandated fields (these shall be defined by the customer as part of system implementation) have been populated;
	- Attach digital Artefacts to Issues and / or Entities and support the following formats:
	  - Pdf files;
	  - Photographs/images (at a minimum .bmp, .jpeg and .png);
	  - Microsoft Office documents.
	- View and make comments on digital Artefacts attached to Issues and / or Entities;
	- Store equipment hazards within the system (as imported from eCassandra in accordance with the AIMS Data Interface Data Dictionaries in the Data Room);
	- Record which equipment hazard a DASOR (see Section A2 Requirement 2 and the DASOR process in the AIMS Process Requirements in the Data Room) relates to;
	- View a summary of all Actions assigned to them, including deadlines and priorities;
	- Search the DES AIMS for Issues, Entities; Artefacts and Actions using key words (free text), record ID, Air System & date ranges (at a minimum);
	- Close or archive an Issue and / or Entity;
	- Re-open a closed or archived Issue and / or Entity;
	- Manage items assigned to them as ‘work in progress’ or draft and noting that these should not be visible to others prior to publication;

	- Publish 'work in progress' or drafts when completed;
	- Link the following AIMS elements:
	  - Artefacts to Issues and / or Entities;
	  - Hazards to Issues and / or Entities (linkage only as part of the DASOR Entity / Process);
	  - Issues to Entities and Entities to Issues;
	  - Issues to Issues.
	- Record any decision of review, amendment or approval with a time/date stamp;
	- Provide comments and / or justification for approvals / decisions;
	- Access chronological audit trail of decisions and evidence underpinning the progression of an Issue;
	- Print content from within AIMS including:
	  - Events and linked elements
	  - Issues and linked elements,
	  - Entity and linked elements,
	  - Artefacts,
	  - Reports;
	- Print Issues and Entities including in standardised formats as appropriate
	- Export a single or multiple Issues and / or Entities in pdf format including all related Artefacts, Issues and Entities including in standardised formats as appropriate.
	- Export a single or multiple Issues and / or Entities in Microsoft Word Document format including all related Artefacts, Issues and Entities including in standardised formats as appropriate.
	- Export a single or multiple Issues and / or Entities in csv format including all related Artefacts, Issues and Entities.
	- Export a single or multiple Issues and / or Entities to a SQL database maintaining the relationship between all AIMS elements (Issues, Entities, Artefacts).
	- Export digital Artefacts in the format they were originally uploaded into AIMS.
	- Export data from the DES AIMS software in accordance with the AIMS Data Interface Data Dictionaries in the Data Room.
	- Import data into the DES AIMS software in accordance with the AIMS Data Interface Data Dictionaries in the Data Room.
	- Download and print standard reports to review Issue and / or Entity progression, ownership and performance.

A.4 – Dashboards and reporting	
1	The Contractor shall provide standard dashboards and reports to provide management information / metrics at: - Operating centre level, covering multiple Air Systems across multiple delivery teams; - TAA level, covering multiple Air Systems across a single delivery team; - Air system level, covering a single Air System; - Authorised User level (summary of all Actions assigned to an individual, including deadlines and priorities). Such standard dashboards and reports shall include as a minimum at each of these levels: - Issue and Entity progression; - Issue and Entity Ownership; - Issue and Entity Performance.
2	The Contractor shall provide standard dashboard reports on-screen, downloadable and printable in both Microsoft Word and pdf formats.
3	The Contractor shall provide the ability to bulk export system usage and performance data in .csv format to support DE&S's internal management information systems and dashboards.
A.5 – System administration functionality	
1	The DES AIMS software shall enable Authorised Users assigned to the system administration role to perform routine system administration tasks via appropriate access permissions without Contractor input. Such tasks shall include, but not be limited to: - Use system administration tools to maintain DES AIMS; - Add, change or remove Authorised Users; - Define and Set permission level groups for Authorised Users; - Conduct archiving activities;

	- Set-up and maintain User look-up lists; - Export bulk data from DES AIMS; - Define, approve and set each Authorised Users permission, authority and access rights.

Part B – The DES AIMS implementation requirement

Serial	Requirement	Payment Mechanism	Critical Acceptance Criteria
B.1 Go-Live			
1	The Contractor shall be responsible for providing the DES AIMS software to meet a Go-live date of the 01 April and in accordance with the Implementation Plan at Schedule 8.	DES AIMS – Go-Live – Milestone 5 as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Go-Live date of 01 April 2019 achieved and accepted by the Authority (including ISS IAtO, Accreditation, training and data migrated). Initial DE&S Authorised User acceptance testing successfully completed to the satisfaction of the Authority
B.2 Data Migration			
1	The Contractor shall migrate the data from the existing supplier managed software system in accordance with the Data Migration Plan at Schedule 8, Annex A. and in line with the DES AIMS Data Migration Extant Position and Future Vision in the Data Room	DES AIMS - All data migrated – Milestone 3 as per Schedule 2, Annex A, Table 1 – Milestone Payments	Confirmation and acceptance by the Authority that the Data Migration has been completed successfully.
2	The Contractor shall import all historical and archived records (from the existing AIMS solution) from provided data files maintaining all relationships between data elements (this shall include any data previously imported (into the existing AIM tool) from other sources). Details of the data to be migrated will be provided at an agreed date during the implementation of DES AIMS.		
3	The Contractor shall ensure all data integrity is maintained without: - missing data; - losing data; and / or - corrupting data.		
4	The Contractor shall provide validation of the migrated data in accordance with the Data Migration Plan at Schedule 8, Annex A.		
5	The Contractor shall provide full audit documentation for data migration to the Authority		
6	The Contractor shall conduct initial population of the DES AIMS with all Authorised Users (as identified by the Authority during the implementation of DES AIMS) to enable them to access the system.		

B.3 Software and network approval			
1	The Contractor shall ensure that DES AIMS conforms to the most recent version of JSP604 Network Joining Rules (an indication of the necessary process for undertaking this is provided within the JSP604 Network Joining Rules Overview in the Data Room). As part of this requirement the Contractor shall provide, at or shortly after contract placement: - a clearly defined high level information exchange document; - a high level network diagram	DES AIMS software and network achieved Interim Approval to Operate (IAtO) – Milestone 1a as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Approval of milestone by the Authority to include: All inputs to JSP604 processes provided in a timely manner. ISS JSP604 – Network Joining Rules approval granted (Authority to Test, Interim Authority to Operate and full Authority to Operate). Full accreditation achieved (including associated RMADS, DART entries and Privacy Impact Assessment (PIA)).
2	The Contractor shall manage the DES AIMS software and network accreditation process in accordance with JSP604, DEF STAN 05-138 ISO 27001/2 principles and industry best practice and demonstrate access from MODNET, DII and across the Assured LAN Interconnect (ALI). This includes the Contractor undertaking any necessary testing and providing documentation to provide evidence in support of the JSP 604 process to achieve an Interim Authority to Operate by 1st April 2019		
3	The Contractor shall provide suitable technically qualified subject matter experts to support, JSP 604 Network Joining Rules and ISS approvals process (including, Authority to Test, Interim Authority to Operate, Full Authority to Operate and associated accreditation processes) prior to the service going live.		
4	The Supplier shall ensure that the DES AIMS service is available with an appropriate level of concurrency of use and accessible from: - MODNET base and overseas capabilities, utilising both desktop and laptop devices; - DII base and overseas capabilities, utilising both desktop and laptop devices; - DII deployed capability (Sys2, Sys4, Minerva) utilising both desktop and laptop devices. - Industry approved devices operating on the MOD Assured LAN Interconnect (ALI).		
5	The Contractor shall ensure that the DES AIMS service is only accessed by approved devices operating on the official DII, MODNET networks or through the Assured LAN Interconnect (ALI) and use DNS (instead of IP address literals) to identify devices and services wherever possible.		
6	The Contractor shall achieve DES AIMS Browser compatibility with the following browser types and versions: - Internet Explorer browser (current version 11.0.9600.19080CO and all later versions) contained within the MODNET build (base and overseas); - Chrome browser (version 64.0.3282.119 and all later versions) contained within the MODNET build (base and overseas);	DES AIMS software and network achieved Interim Approval to Operate (IAtO) – Milestone 1a as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Approval of milestone by the Authority to include: All inputs to JSP604 processes provided in a timely manner. ISS JSP604 – Network Joining

	- Internet Explorer browser (current version 11.0.9600.19080CO and all later versions) contained within the DII build (base, overseas and deployed); - Chrome browser (current version 64.0.3282.119 and all later versions) contained within the DI build (base, overseas and deployed).		Rules approval granted (Authority to Test, Interim Authority to Operate and full Authority to Operate). Full accreditation achieved (including associated RMADS, DART entries and Privacy Impact Assessment (PIA)).
7	The Contractor shall achieve DES AIMS Browser compatibility with the following browser types and versions: - Internet Explorer browser (version assumed to be newer than DII / MODNET version) running on Industry owned approved devices operating on the official network (via the Assured LAN Interconnect (ALI)); - Chrome browser (version assumed to be newer than DII / MODNET version) running on Industry owned approved devices operating on the official network (via the ALI).		
8	The Contractor shall ensure that the DE&S Airworthiness Issue Management System complies with MOD Domain Name Space Hierarchy and relevant MOD policy leaflets (as per the MoD DNS Policy Leaflet in the Data Room) for all implementation.	DES AIMS software and network achieved Interim Approval to Operate (IAtO) – Milestone 1a as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Approval of milestone by the Authority to include: All inputs to JSP604 processes provided in a timely manner. ISS JSP604 – Network Joining Rules approval granted (Authority to Test, Interim Authority to Operate and full Authority to Operate). Full accreditation achieved (including associated RMADS, DART entries and Privacy Impact Assessment (PIA)).
9	The Contractor shall demonstrate compliance with all relevant safety legislation, regulations and standards including as a minimum JSP430, JSP454 and Def Stan 00-56.		
10	The Contractor is responsible for engaging with the appropriate accreditation process to enable the DES AIMS system (including software, infrastructure and hosting environment) to achieve accreditation prior to go-live.		
11	The Contractor shall demonstrate compliance with Cyber Essentials		
12	The Contractor shall provide a Business Continuity and Disaster Recovery Plan in accordance with Part C.5 - Business continuity and disaster recovery requirement.		
13	The Contractor shall provide a secure backup capability to enable restoration of MoD information in accordance with the Business Continuity and Disaster Recovery Plan.		
14	The Contractor shall operate, manage and host the DES AIMS service from the UK and in UK based data centre(s) and within the MOD network boundary (most likely within Authority Zone 2a; to be confirmed during the execution of JSP604 processes).		
15	The Contractor shall operate the DES AIMS service to handle 'Official-Sensitive' data defined in accordance with JSP440 Part 4.		
16	The Contractor shall manage the DES AIMS software and network accreditation process in accordance with JSP604, DEF STAN 05-138 ISO 27001/2 principles and industry best practice and demonstrate access from	DES AIMS software and network achieved full Approval to Operate (AtO) –	Approval of milestone by the Authority to include: All inputs to JSP604

	MODNET, DII and across the Assured LAN Interconnect (ALI). This includes the Contractor undertaking any necessary testing and providing documentation to provide evidence in support of the JSP 604 process to achieve an Authority to Operate no later than 01 October 2019.	Milestone 1b as per Schedule 2, Annex A, Table 1 – Milestone Payments.	processes provided in a timely manner. ISS JSP604 – Network Joining Rules Approval to Operate granted.

B.4 Configuration			
1	The Contractor shall provide and configure the DES AIMS software in accordance with the Software Configuration Plan as per Annex B to Schedule 8 and to ensure compliance with: - MAA Regulations; - Air Environment policy; - Internal DE&S procedures; and as determined during the ITT process.	DES AIMS software configuration complete – Milestone 2 as per Schedule 2, Annex A, Table 1 – Milestone Payments	Confirmation and approval by the Authority that the system has been configured to allow Authorised Users to use the DES AIMS to meet the Part A DES software requirement. This should include: - an implementation report (capturing any key issues arising and outstanding issues at the end of implementation) - successful initial DE&S User Testing to include validation of Authorised User access permissions.
2	The Contractor shall conduct testing services on the configured DES AIMS software in accordance with the Software Configuration Plan as per Annex B to Schedule 8 and to ensure compliance with: - MAA Regulations; - Air Environment policy; - Internal DE&S procedures; and as determined during the ITT process.		
3	The Contractor shall configure and successfully test import and export functionality in accordance with the AIMS Data Interface Data Dictionaries in the Data Room and the Software Configuration Plan as per Annex B to Schedule 8.		
4	The Contractor shall configure and successfully test MOD standardised formats for both printing and exporting data from the DES AIMS software in accordance with the formats provided as part of the process descriptions (see the AIM Process Requirements in the Data Room), the MRP and in accordance with the Software Configuration Plan as per Annex B to Schedule 8.		
5	The DES AIMS software shall be configured to enable Authorised User Access permissions in accordance with the DES AIMS Access Strategy (in the Data Room) and the Software Configuration Plan as per Annex B to Schedule 8. Role permission profiles will be provided by the Authority during the implementation of DES AIMS.		
B.5 User Readiness and training			
1	The Contractor's responsibilities shall include provision of initial training, for all 6,300 Authorised Users in accordance with the Training Plan using appropriate training methods and approaches to enable Authorised Users to competently operate the DES AIMS software. The Contractor shall ensure that Authorised Users have sufficient awareness and / or training to enable them to access and use the DES AIMS from 01 April 2019 and in accordance with the DES AIMS Training Plan at Schedule 9. Competence is defined here as the ability to operate the system effectively and efficiently, as appropriate to the individual's role without supervision in accordance with	As per Milestone 4a and 4b	See 4a and 4b below.

	the User and System functionality as specified in this SOR. The Contractor shall tailor training to roles and enable Authorised Users to manage Events, Issues and Entities without supervision. The Contractors training methods shall include (but not be limited to): - online training in accordance with UK Government Assisted Digital Guidance and accredited where required within the Government Digital by Default Services Standard and accessible from the MoD Network and end user devices (**Note: Online training will need to be tested and authorised for access across the MoD Networks**); - Integrated user guides both for Authorised Users and Authorised Users in the system administration role include supporting on screen prompts; - Provision of SCORM training packages for DE&S to host and utilise for training of Authorised Users; face to face training.		
2	A minimum of 25% of Authorised Users (as specified by the Authority prior to commencement of the training) shall be trained to operate the system competently by 01 April 2019.	DES AIMS adopted: Initial training complete – Milestone 4a 2 as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Confirmation and evidence by the Contractor that 25% of Authorised Users have been trained to use DES AIMS and appropriate feedback to provide evidence that they are able to operate the system competently.
3	The Contractor shall ensure that the remaining Authorised Users have sufficient awareness and / or training to enable them to access and use the DES AIMS by 01 October 2019 and in accordance with the DES AIMS Training Plan at Schedule 9.	DES AIMS adopted: Full training complete – Milestone 4b 2 as per Schedule 2, Annex A, Table 1 – Milestone Payments.	Confirmation and evidence by the Contractor that the remaining Authorised Users have been trained to use DES AIMS and appropriate feedback to provide evidence that they are able to operate the system competently.
4	The Contractor shall include in their Training Plan the requirement for New User and top training as per Schedule 2, Part C.8 – New User and top-up training.	See C.8 below.	N/A

Part C – The DES AIMS service requirement

Serial	Requirement	Payment Mechanism	Critical Acceptance Criteria
C.1 – Service			
1	The Contractor shall provide a fully accredited DES AIMS service as a managed application service with access from MoD accredited, network attached, devices in accordance with JSP 604, DEF STAN 05-138, ISO 27001/2 principles and industry best practice. This includes the provision of suitable, technically qualified subject matter experts to maintain accreditation over the life of the contract.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service.	Accreditation maintained in accordance with the ISS Authority to Operate and the SLA.
2	The Contractor shall ensure that the DES AIMS software shall remain compliant with MAA Regulations and Air Environment policy throughout the duration of the Contract. This shall include any necessary configuration of the DES AIMS software.		Monthly review in accordance with the SLA. Monthly report agreed and authorised by the Authority.
3	The Contractor shall not access data held on DES AIMS in the operation of the DES AIMS service provision but shall enable Authorised Users to access and handle data held on DES AIMS.		
C.2 – Technical support			
1	The Contractor shall provide a DES AIMS support helpdesk for all Authorised Users between the hours of service operation in accordance with the SLA at Annex A to Schedule 11, Monday to Friday (excluding Bank Holidays) via telephone.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service.	Monthly review in accordance with the SLA. Monthly report agreed and authorised by the Authority.
2	The Contractor shall provide an online support facility on 24/7 basis which as a minimum allows Authorised Users to raise incidents, obtain information on major outages and on planned maintenance.		
3	The Contractor shall provide a Single Point of Contact (SPoC).		
4	The Contractor shall provide technical support to resolve service incidents, problems and requests (terms as defined by ITIL) on a 24/7 basis.		
5	The Contractor shall provide all levels of technical application and infrastructure support (1st, 2nd, 3rd line)		
6	The Contractor shall apply Information Technology Infrastructure Library (ITIL 2011) best practices, including incident, problem and change management to minimize the risk of recurring problems and negative Authorised User impacts.		
C.3 - Service levels			
1	The Contractor shall provide the DES AIMS service on a 24 hour basis, 365 days-a-year with an agreed availability measured in accordance with the Service Level Agreement at Annex A to Schedule 11 to 6,300 Authorised Users at the agreed concurrency of use. Availability here shall be defined as full functionality of the toolset being available to all Authorised Users, in all locations at agreed performance levels.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Monthly review in accordance with the SLA. Monthly report agreed and authorised by the Authority.
2	The Contractor shall maintain a minimum performance level, meaning here the ability to access and use DES AIMS, as per the Service Level		

	Agreement at Annex A to Schedule 11 and is bound by any agreed constraints (such as concurrent Users and boundaries of responsibility) where the level is consistent with reasonable expectations of business usage of the service and in accordance with the User Journeys detailed in the Data Room;		
3	The Contractor shall maintain incident resolution times in accordance with the Service Level Agreement at Annex A of Schedule 11.		
4	The Contractor shall use active system monitoring and alerting for service availability, infrastructure, data replication and security breaches (at a minimum).		
5	The Contractor shall provide and maintain the DES AIMS service in accordance with the Service Level Agreement at Annex A to Schedule 11.		
6	The Contractor shall maintain User access control in accordance with Schedule 15.		
7	The Contractor shall be able to scale the DES AIMS service up or down in 50 Authorised User increments.	Monthly Service Fee adjustment in accordance Schedule 2, Annex A, Table 3 – DES AIMS service – price per User.	
C.4 - System Administration Support			
1	The Contractor shall provide full system administration support services covering all system administration activities to all Authorised Users.	Monthly system administration support service Fee in accordance Schedule 2, Table 2 – DES AIMS system administration support service fee.	Monthly review of the performance of the administration service in accordance with the SLA
2	The Contractor shall monitor and report performance of the system administration support service in accordance with the System Administration Service Level Agreement as per Annex B to Schedule 11.		
3	The Contractor shall make provision for the Authority to take over the System Administration Support services over the life of the DES AIMS service.		
4	The Contractor shall be able to scale the DES AIMS system administration support services up or down.	Monthly system administration support service Fee adjustment in accordance Schedule 2, Annex A, Table 4 – DES AIMS system administration support service – price per User.	Monthly review of the administration service in accordance with the SLA. Any reductions agreed between the Authority and the Contractor.
C.5 - Business continuity and disaster recovery			
1	The Contractor shall maintain a business continuity and disaster recovery process, and make this available for review by the Authority, in accordance with the Business Continuity and Disaster Recovery Plan at Annex A to Schedule 12 throughout the life of the contract.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Successful Disaster Recovery Simulation (at least once per contract year)

2	The Contractor shall conduct and report against at least one successful disaster recovery simulation every Contract Year, against the stated RPO and RTO, in accordance with the Business Continuity and Disaster Recovery Plan.		Simulation Report including recommendations and proposed rectifications provided to the Authority in accordance with the requirement and the SLA within 10 working days of the successful completion of the simulation Authority acceptance of the Simulation Report
3	The Contractor shall provide business continuity and disaster recovery services based upon: - A Recovery Point Objective (RPO) of 12 hours (100% of service capability and data recovered) applying to the point at which incident or loss occurs; - A Recovery Time Objective (RTO) of 24 hours or 7 working hours (whichever is lesser) to restore to the agreed RPO or better.		
4	The Contractor shall maintain a disaster recovery capability sufficient to restore the DES AIMS service to the RPO within the stated RTO.		
5	The Contractor shall invoke the disaster recovery capability when requested by the Authorities named POCs.		
6	The Contractor shall maintain the capability to securely backup information and enable its restoration in the event of business interruptions or disasters including security related incidents and data protection breaches.		Monthly service review delivered in accordance with the SLA
7	The DES AIMS service shall receive: - critical security patches within two weeks; - non-critical security patches at a minimum of every six months.; - major functional upgrades at a minimum once per year in agreement with the Authority; - incremental upgrades as needed for fault resolution of incidents of Priority 3 and above.		
8	The Contractor shall inform the Authority about incidents within 1 hour of occurrence (as defined by active monitoring or incident) with notifications delivered via email to the nominated DE&S point(s) of contact or mailbox(es). Points of Contact will be nominated by the Authority during the Implementation phase.		
9	The Contractor shall inform the Authority about security incidents within 20 minutes of occurrence (as defined by active monitoring or incident) with notifications delivered via email to the nominated DE&S point(s) of contact or mailbox(es). Points of Contact will be nominated by the Authority during the implementation of DES AIMS.		
C.6 - Contract Management and Reporting			
1	The Contractor shall attend monthly contract management and meetings at the Authority's offices.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Monthly service reviews conducted with the Authority. Authority approval of the minutes of the service review within 5 working days of the review.
2	The Contractor shall provide monthly service	Monthly	Monthly service

	performance reports within 10 working days of the end of the month to include comprehensive data about the services provided under Part C – DES AIMS service to reflect the SLA as per Annex A of Schedule 11 and DES AIMS system administration SLA as per Annex B of Schedule 11.	Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee and monthly system administration support service Fee in accordance Schedule 2, Table 4 – DES AIMS system administration support service fee.	report agreed with the Authority. The report must contain all service performance details in accordance with the SLA and the system administration SLA.
C.7 - Exit Strategy			
1	The Contractor shall maintain an Exit Plan at Annex A to Schedule 10.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Reviewed as part of a relevant Monthly Review
C.8 – New User and top-up training			
1	The Contractor's responsibilities shall include provision of training for up to 1,500 new Authorised Users, per contractual year, in accordance with the Training Plan at Schedule 9. This shall be conducted using appropriate training methods and approaches to enable Authorised Users to operate the DES AIMS competently.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Monthly Service Reviews Review of conducted training as part of Monthly Reviews
2	The Contractor shall provide top-up training to all Authorised Users, where changes are made to the DES AIMS software, in accordance with the Training Plan using appropriate training methods and approaches for any new features and / or services being provided on the DES AIMS.	Monthly Service Fee in accordance Schedule 2, Annex A, Table 2 – DES AIMS service fee.	Monthly Service Reviews Review of conducted top-up training and proposed upcoming required top-up training as part of Monthly Reviews
C.9 - Additional Services			
1	The Contractor shall provide additional DE&S Airworthiness Issue Management Services as per the Additional Tasking Process at Schedule 13. The scope of that work includes: - Interface and data uploading services; - Configuration services; - Training services including face-to-face and tailored training materials, - Data migration services; - Data archiving services; - Technical subject matter expertise; MoD Data processing activities (this shall include the need for Contractor employees shall sign a DEFFORM 702 (Employee's Acknowledgement to Employer of Obligations Relating to Confidentiality) where any MoD data will need to be processed)	As per the additional tasking process and based on the Rate Card as per Annex B of Schedule 13.	As per the additional tasking process tasking order forms.

Part D –DES AIMS supporting requirements

Serial	Requirement	Payment Mechanism	Critical Acceptance Criteria
1	All Contractor personnel working on the DES AIMS must be UK based and SC cleared (or if working towards this must have basic level clearance (BPSS)). Clearance details must be provided to the Authority for review and confirmation prior to the commencement of the service.	N/A	All Staff cleared as per the requirement.

Annex A to Schedule 2

Pricing of Schedule of Requirements for Contract No: CCDT/491

For: Airworthiness Issues Management System

Table 1 – Milestone Payments (exluding VAT)

Taken from ITT response:

Milestone	Description	Critical Acceptance Criteria (to be approved by the Authority)	Milestone Payment
1a	DES AIMS software and network achieved Interim Approval to Operate	- All inputs to JSP604 processes provided in a timely manner. - ISS JSP604 – Network Joining Rules approval granted (Authority to Test, Interim Authority to Operate and full Authority to Operate). Full accreditation achieved (including associated RMADS, DART entries and Privacy Impact Assessment (PIA)).	**[Redacted]**
1b	DES AIMS software and network achieved full Approval to Operate	- All inputs to JSP604 processes provided in a timely manner. - ISS JSP604 – Network Joining Rules Approval to Operate granted by 01 October 2019.	**[Redacted]**
2	DES AIMS software configuration complete	- Confirmation and approval by the Authority that the system has been configured to allow Authorised Users to use the DES AIMS to meet the Part A DES software requirement. This should include: - an implementation report (capturing any key issues arising and outstanding issues at the end of implementation) - successful initial DE&S User Testing to include validation of Authorised User access permissions.	**[Redacted]**
3	DES AIMS - All data migrated	- Confirmation and acceptance by the Authority that the Data Migration has been completed successfully.	**[Redacted]**
4a	DES AIMS adopted: Initial training complete	- Confirmation and evidence by the Contractor that 25% of Authorised Users have been trained to use DES AIMS and appropriate feedback to provide evidence that they are able to operate the system competently.	**[Redacted]**
4b	DES AIMS adopted: Full training complete	- Confirmation and evidence by the Contractor that the remaining Authorised Users have been trained to use DES AIMS and appropriate feedback to provide evidence that they are able to operate the system competently.	**[Redacted]**
5	DES AIMS – Go-Live – Milestone 5	- Go-Live date achieved and accepted by the Authority (including ISS IAtO, Accreditation, training and data migrated). Initial DE&S Authorised User acceptance testing successfully completed to the satisfaction of the Authority	**[Redacted]**
Total Part B Firm Price			**[Redacted]**

Table 2 – DES AIMS Service Fee (excluding VAT)

Year 1 - 2				
Item	Number of Authorised Users *	Price Per User/Per Months	Monthly DES AIMS Service Fee	Total Price (for 24 months)
(A)	(B)	(C)	(D)	(E)
Provision of a DES AIMS service in accordance with Schedule 2, Part C excluding C.4 system administration support services and C.8 additional services.	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Provision of a DES AIMS system administration support service as per Schedule 2, Part C.4.	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Total Year 1 – 2 (excluding VAT)				**[Redacted]**
Option Year 1				
Item	Number of Authorised Users	Price Per User/Per Months	Monthly DES AIMS Service Fee	Total Price (for 24 months)
(A)	(B)	(C)	(D)	(E)
Provision of a DES AIMS service in accordance with Schedule 2, Part C excluding C.4 system administration support services and C.8 additional services	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Provision of a DES AIMS system administration support service as per Schedule 2, Part C.4.	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Total Option Year 1 (excluding VAT)				**[Redacted]**
Option Year 2				
Item	Number of Authorised Users	Price Per User/Per Months	Monthly DES AIMS Service Fee	Total Price (for 24 months)
(A)	(B)	(C)	(D)	(E)
Provision of a DES AIMS service in accordance with Schedule 2, Part C excluding C.4 system administration support services and C.8 additional services	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Provision of a DES AIMS system administration support service as per Schedule 2, Part C.4.	**[Redacted]**	**[Redacted]**	**[Redacted]**	**[Redacted]**
Total Option Year 2 (excluding VAT)				**[Redacted]**
Total Part C Firm Price Cost Proposal (excluding VAT)				**[Redacted]**

[Redacted]

Table 3 – DES AIMS Service – Price Per User (excluding VAT)

DES AIMS Service Authorised Users	Price Per User/Per Months
(A) TIERED PRICING	(B)
0 – 250	**[Redacted]**
251 – 500	**[Redacted]**
501 – 1,000	**[Redacted]**
1,001 – 3,000	**[Redacted]**
3,001 – 5,000	**[Redacted]**
5,001 – 7,500	**[Redacted]**
7,501 – 10,000	**[Redacted]**
10,001 – 20,000	**[Redacted]**

Table 4 – DES AIMS System Administration Support Service Fee (excluding VAT)

DES AIMS system administration support services provided to Authorised Users	Price Per User/Per Months
(A) TIERED PRICING	(B)
0 – 250	**[Redacted]**
251 – 500	**[Redacted]**
501 – 1,000	**[Redacted]**
1,001 – 3,000	**[Redacted]**
3,001 – 5,000	**[Redacted]**
5,001 – 7,500	**[Redacted]**
7,501 – 10,000	**[Redacted]**
10,001 – 20,000	**[Redacted]**

Annex B to Schedule 2 – Authority Dependencies & GFX

Dep No	Dependency / GFX Title	Description	Remarks
1.	AIMS Data	The Authority is required to provide all necessary AIMS data where this is not already held on the Contractor's Resolve system.	
2.	Authority Data SME	The Authority is required to appoint a representative or Delivery Team (DT) specific representative who has extensive knowledge of the local DT data. This individual is required to be assigned at Contract Start. This individual will need to be accessible to the Contractor personnel as required to clear impediments.	
3.	Go-Live Authority	The Authority is required to designate a Go-Live Authority responsible for authorising Go-Live at Contract Start. This individual will need to be available in order to support the data migration plan including providing agreement for the Contractor to temporarily take RESOLVE off-line during Go-Live if required.	
4.	AIMS Data	The required AIMS data format to be migrated is required to remain in a stable structure from Contract Start. The Authority is required to support an agreed data snapshot date prior to final migration no later than 10 Working Days before the Go-Live date.	
5.	Authority Configuration SME	The Authority is required to appoint a representative to oversee and adjudicate on software configuration changes on behalf of all DTs and act as PoC. This individual is required to be assigned at Contract Start in order to initiate process coherence activity. This individual will need to be accessible to the Contractor personnel as required to clear impediments.	
6.	Access to eCassandra Hazards Data	In order to enable AIMS interface testing and configuration, the Contractor is required to be provided with all necessary eCassandra Hazards Data in a stable Hazard Log format no later than 15 April 2019 for all DTs/Air Systems. Any changes after this date will be modified as part of ongoing service after Go-Live and not disrupt the Go-Live schedule.	
7.	Additional OC and TAA Reporting	Any new reports or reports requiring additional configuration before Go-Live will approved and signed off by the Authority and supplied no later than the 01 April 2019. Any requirements after this date will be provided in accordance with ongoing service after Go-Live and not disrupt the Go-Live schedule.	
8.	Customer Site Training Rooms	Rooms to be provided at Customer main sites for the purposes of delivering DES AIMS F2F training by the Contractor trainers. Room to meet capacity of delegates required (not to exceed twenty) and include for: • Screen Projector to connect to Trainer laptop. • Screen. • Tables/Desks for all Delegates.	

Dep No	Dependency / GFX Title	Description	Remarks
9.	Customer Site Training Rooms - Booking	Where DES AIMS training is required on site then Customer Site Training Rooms are to be provided (booked) by the Authority's representative (DES AIMS Local (Training) Co-ordinator) not less than FOUR weeks prior to the agreed training date.	
10.	Customer Site Training – Access	Where DES AIMS training is required on a Customer Site then the Authority's representative (DES AIMS Local (Training) Co-ordinator) is required to facilitate access to the site/room for the Contractor DES AIMS Trainer(s).	
11.	Customer Site Training – Delegates	Where DES AIMS training is required on a Customer Site then the Authority's representative (DES AIMS Local (Training) Co-ordinator) is responsible for ensuring all delegates are advised of the training location/date/time and any specific access arrangements they may require.	
12.	Online Training – Advertisement	Where the Authorised User community are required to complete Online Training as part of the DES AIMS Alignment Training activity then from 01 Feb 19 the Authority is required to assist the Contractor efforts to advertise the existence of the course and the need for completion prior to Go-Live.	
13.	Authority verification of Service Requests.	Approval of all Service Requests shall be provided by the Authority, prior to submission to the Contractor.	Ensures Authorised Users are permitted to hold the levels of access requested and have legitimate business reasons to do so.
14.	Removal of User accounts.	A Service Request shall be raised by the Authority once each month, providing a consolidated list of Authorised User accounts to be removed.	
15.	Permission-level Groups.	The parameters for permission-level Groups shall be approved by a designated Authority representative, prior to the Service desk applying the necessary actions.	
16.	Achieving DES AIMS Accreditation – Cyber Risk Profile	The Authority is required to provide the Cyber Risk Profile for the DES AIMS within five business days after contract startcommencement.	

Annex C to Schedule 2 – Contractor Key Roles

The Contractor has extensive skills and experience which we believe significantly increase the chances of success of the programme and reduce the dependencies on the Authority. The Contractor employs people who have previously held senior roles in the MOD and in the defence industry working across the Military Aviation Environment (MAE); specifically in the engineering, safety and airworthiness functions. Their knowledge is augmented by professional qualifications up to Master's Degree level in related subjects, including Safety Management. Certain individuals have previously been issued DE&S Letters of Airworthiness Authority (LoAA), while others have been appointed as Air System Safety Managers. The Contractor believes that this experience will assist the Authority by not only providing a more assured quality solution, but also by reducing the requirement for Authority assistance.

Additionally, the Contractor team of software technical and IT network professionals have a wealth of experience of Airworthiness Issues Management Systems (AIMS) from working within the Contractor's organisation. The accumulated software and IT experience they are able to bring to this programme is significant and possibly unrivalled in the UK within AIMS.

Contractor Key Roles, Resources

The Contractor Integration Manager shall be responsible for service transition activity, including change management, supporting Authority workshops and providing Subject Matter Expert (SME) advice. This resource will be act as a Point of contact (PoC) between the Contractor and the Authority

The Contractor Senior Information Risk Officer (SIRO) shall be responsible for managing all information risks across the Contractor's organisation and is accountable to the Contractor Board of Directors. The SIRO owns the overall Information Risk Policy and ensures that information risk assessments are done taking account of internal and external guidance and regulation. The SIRO is point of escalation for all data related concerns of the team involved in data migration. SIRO will be the Company PoC offering advice in the event of a potential ISO270001/BS10008 breach or tasking demand. This includes, assurance that the Organisation is compliant with all the relevant statutory, regulatory and other mandatory measures to safeguard information and associated Information Assets. The SIRO advises the Contractor Information Asset Owner (IAO) on all information risk aspects of the information assets.

Contractor Information Asset Owner (IAO)

The IAO is responsible for managing the risks to all information assets, and ensuring that all information assets are protected and shared appropriately in order to comply with MOD Policy, Contractor Processes and current UK legislation. The IAO is able to understand and address the risks associated with the information assets they are responsible for. Operationally, they are responsible for ensuring that access controls to Information Assets allows business to be conducted with an acceptable level of risk. The IAO provides detailed reports to the SIRO on all Information Assets in the Contractor's custody.

The Contractor Security Working Group (SWG) is an autonomous body that act in the best interests of the Contractor with its ultimate aim to up-hold the Contractor's Security Objectives and to provide timely security related information to the wider stakeholder community. The SWG acts as the authority for all information security issues across the Contactor's organisation and

provides knowledge, training and expertise to the wider Contractor's organisation on all matters relating to Information Security, Cyber, Secure Development, Physical and Technical Assurance. The SWG will ensure appropriate levels of Confidentiality, Integrity, Availability and Authenticity (CIAA) of Information Assets are maintained.

The Contractor Airworthiness and Safety Working Group (tASWG) is an independent body that act in the best interests of the Contractor with its ultimate aim to up-hold the Contractor's Safety Objectives and to provide timely safety and airworthiness information related information to the wider stakeholder community. The tASWG acts as the authority for all safety and airworthiness issues across the Contactor's organisation and provides knowledge, training and expertise to the wider Contractor's organisation on all such matters.

The Contactor Integration Manager shall be responsible for service transition activity, including change management, supporting Authority workshops and providing SME advice. This resource will be act as a PoC between the Contractor and the Authority.

The DES AIMS Trainer(s) shall be responsible for tailoring, designing, updating, scheduling and delivery of the DES AIMS User Readiness Training.

Annex D to Schedule 2 – Contractor Assumptions & Constraints

The Contractor secure zone 2a accredited network is a suitable environment in which to handle data.

Achieving DES AIMS Accreditation – DIAS - It is assumed that the DES AIMS will require a full Defence Information Assurance and Security (DIAS) assessment.

Data Migration Training, F2F – Capacity -
F2F training provide by the Contractor not to exceed 20 delegates per course, unless by prior agreement.

Annex E to Schedule 2 – Contractor Exclusions

ID	Exclusion Title	Description	Remarks
1.	Data Migration Training, F2F – Low Attendance	Attendance to F2F Training courses by the Contractor DES AIMS trainers is excluded where the minimum delegate attendance level of five is not achievable, unless by prior agreement.	
2.	New User F2F Training – Monthly Capacity	Capacity for New User F2F training courses provided by the Contractor DES AIMS trainers will not exceed 180 delegate places per month.	
3.	New User accounts.	The bulk creation of new Authorised User accounts (e.g. during the introduction of an additional Air System and/or DT to DES AIMS) shall be excluded from Service Request SLA performance reporting metrics.	
4.	Permission-level Groups.	Large-scale changes to permission-level Groups shall be considered non-routine and excluded from performance reporting metrics.	Resulting from Authority organisational changes, unless as a result of changes to MAA Regulations or Air Environment Policy.
5.	Look-up List changes.	Service Requests for amendments to look-up lists that have a significant data integrity impact shall be excluded from SLA performance reporting metrics	Removal of existing items in a look-up list that may have been selected by Users within a DES AIMS entity could affect the integrity of related data and require a greater depth of resolution.
6.	Bulk data export request.	Any request for the bulk export of the complete DES AIMS database export shall be requested separately by the Authority to the Contractor and not included within the SLA performance reporting metrics.	At any point throughout the contract period, the Contractor shall “provide all DE&S data and attachments in an SQL Server format database within 10 working days of a request”.
7.	Non-routine Service Requests.	Non-routine Service Requests shall be excluded from performance reporting metrics.	Large-scale exceptional requests.
8.	Out-of-scope Service Request.	A System Administration Service Request deemed to be a Training Requirement, or Incident Report, or Additional Service shall be excluded from the System Administration Support SLA metrics.	
9.	SLA failures	the Contractor shall not to be penalised for service level failures that are outside its control.	
10.	Downtime for non-Contractor controlled systems	Downtime for other systems (DTOS) outside the control of the Contractor (i.e. MODNET) that affect DES AIMS operation whether planned or unplanned is excluded from the performance metrics	The Contractor monitors notifications from the GOSCC Planned Outage Cell and will notify Authorised Users when any outage will affect the DES AIMS service.
11.	Service Availability	Any Planned Downtime is excluded from the Availability calculations	

Schedule 3 – Contract Data Sheet

General Conditions
Condition 2 – Duration of Contract: The contract commencement date shall be: Part B – The DES AIMS implementation requirement: **04 March 2019 and expire upon delivery and acceptance of all Milestones** as per Table 1 – Milestone Payments on the basis of the prices set out in Annex A to Schedule 2 (Pricing of Schedule of Requirements for Contract No CCDT/491 – Table 1 – Milestone Payments. Part C – The DES AIMS Service requirement: **01 April 2019. The Contract expiry date shall be: 31 March 2021** with unilateral options, exercisable by the Authority, to extend for a further year to 31 March 2022 and thereafter for a further year to 31 March 2023 on the basis of the prices set out in Annex A to Schedule 2 (Pricing of Schedule of Requirements for Contract No: CCDT/491 – Table2 DES AIMS Service Fee, Table 3 DES AIMS Service Price per User and Table 4 DES AIMS System Administration Support Service Fee).
Condition 4 – Governing Law: Contract to be governed and construed in accordance with: English Law ☒ Scots Law ☐ clause 4.d shall apply *(one must be chosen)* Solicitors or other persons based in England and Wales (or Scotland if Scots Law applies) irrevocably appointed for Contractors without a place of business in England (or Scotland, if Scots Law applies) in accordance with clause 4.g (if applicable) are as follows:
Condition 8 – Authority's Representatives: The Authority's Representatives for the Contract are as follows: Commercial: Kimrun Sooriya *(as per DEFFORM 111)* Project Manager: - Part B – Nick Hillier-Smith - Part C – Jonathan Higgins *(as per DEFFORM 111)*
Condition 19 – Notices: Notices served under the Contract shall be sent to the following address: Authority: CCDT, Spruce 2B, Abbey Wood, Bristol, BS34 8JH Contractor: tlmNexus Notices can be sent by electronic mail? ☒ *(tick as appropriate)*

Condition 20.a – Progress Meetings:

The Contractor shall be required to attend the following meetings:

Monthly contract management meetings held at ABW
Annual review to be held at ABW

Condition 20.b – Progress Reports:

The Contractor is required to submit the following Reports:

As per Schedule 2.

Supply of Contractor Deliverables

Condition 21 – Quality Assurance: Not Applicable

Is a Deliverable Quality Plan required for this Contract? ☐ *(tick as appropriate)*

If required, the Deliverable Quality Plan must be set out as defined in AQAP 2105 and delivered to the Authority (Quality) within Business Days of Contract Award. Once agreed by the Authority the Quality Plan shall be incorporated into the Contract. The Contractor shall remain at all times solely responsible for the accuracy, suitability and applicability of the Deliverable Quality Plan.

Other Quality Assurance Requirements:

Condition 22 – Marking of Contractor Deliverables:

Special Marking requirements:

Not Applicable

Condition 24 - Supply of Data for Hazardous Contractor Deliverables, Materials and Substances: Not Applicable

A completed Schedule 6 (Hazardous Contractor Deliverables, Materials or Substance Statement), and if applicable, Safety Data Sheet(s) are to be provided by e-mail with attachments in Adobe PDF or MS WORD format to:

a) The Authority's Representative (Commercial)

b) Defence Safety Authority – DSA-DLSR-MovTpt-DGHSIS@mod.uk

to be Delivered no later than one (1) month prior to the Delivery Date for the Contract Deliverable or by the following date:

Condition 25 – Timber and Wood-Derived Products: Not Applicable

A completed Schedule 7 (Timber and Wood-Derived Products Supplied under the Contract: Data Requirements) is to be provided by e-mail with attachments in Adobe PDF or MS WORD format to the Authority's Representative (Commercial)

to be Delivered by the following date:

Condition 26 – Certificate of Conformity: Not Applicable

Is a Certificate of Conformity required for this Contract? ☐ *(tick as appropriate)*

Applicable to Line Items:

If required, does the Contractor Deliverables require traceability throughout the supply chain? ☐ *(tick as appropriate)*

Applicable to Line Items:

Condition 28.b – Delivery by the Contractor:

The following Line Items are to be Delivered by the Contractor:

In accordance with Schedule 2 – Statement of Requirements

Special Delivery Instructions:

Not Applicable.

Each consignment is to be accompanied by a DEFFORM 129J.

Condition 28.c - Collection by the Authority: Not Applicable

The following Line Items are to be Collected by the Authority:

Special Delivery Instructions:

Each consignment is to be accompanied by a DEFFORM 129J.

Consignor details (in accordance with 28.c.(4)):

Line Items: Address:

Line Items: Address:

Consignee details (in accordance with condition 23):

Line Items: Address:

Line Items: Address:

Condition 30 – Rejection:

The default time limit for rejection of the Contractor Deliverables is thirty (30) days unless otherwise specified here:

The time limit for rejection shall be Business Days.

Condition 32 – Self-to-Self Delivery: Not Applicable

Self-to-Self Delivery required? ☐ *(tick as appropriate)*

If required, Delivery address applicable:

Pricing and Payment
Condition 35 – Contract Price: All Schedule 2 line items shall be Firm Price other than those stated below: Line Items Clause 46. refers

Termination
Condition 42 – Termination for Convenience: The Notice period for terminating the Contract shall be twenty (20) days unless otherwise specified here: The Notice period for termination shall be __ Business Days

Other Addresses and Other Information *(forms and publications addresses and official use information)*
See Annex A to Schedule 3 (DEFFORM 111)

Schedule 4 Appendix - Addresses and Other Information

DEFFORM 111
(Edn 12/17)

1. Commercial Officer

Name: Kimrun Sooriya

Address: Abbey Wood, Bristol

Email: Kimrun.Sooriya101@mod.gov.uk

2. Project Manager, Equipment Support Manager or PT Leader
(from whom technical information is available)
Name: Mr Jonathan Higgins
Address Abbey Wood, Bristol

Email: Jonathan.Higgins108@mod.gov.uk

3. Packaging Design Authority – Not Applicable

Organisation & point of contact:

(Where no address is shown please contact the Project Team in Box 2)

4. (a) Supply / Support Management Branch or Order Manager:
Branch/Name:

Tel No:

(b) U.I.N.

5. Drawings/Specifications are available from

6. INTENTIONALLY BLANK

8. Public Accounting Authority

1. Returns under DEFCON 694 (or SC equivalent) should be sent to DBS Finance ADMT – Assets In Industry 1, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
☎ 44 (0) 161 233 5397

2. For all other enquiries contact DES Fin FA-AMET Policy, Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
☎ 44 (0) 161 233 5394

9. Consignment Instructions

The items are to be consigned as follows:

10. Transport. The appropriate Ministry of Defence Transport Offices are:
A. DSCOM, DE&S, DSCOM, MoD Abbey Wood, Cedar 3c, Mail Point 3351, BRISTOL BS34 8JH
Air Freight Centre
IMPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943
EXPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943
Surface Freight Centre
IMPORTS ☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
EXPORTS ☎ 030 679 81129 / 81133 / 81138 Fax 0117 913 8946
B. JSCS

JSCS Helpdesk No. 01869 256052 (select option 2, then option 3) JSCS Fax No. 01869 256837
www.freightcollection.com

11. The Invoice Paying Authority
Ministry of Defence ☎ 0151-242-2000
DBS Finance
Walker House, Exchange Flags Fax: 0151-242-2809
Liverpool, L2 3YL **Website is:**
https://www.gov.uk/government/organisations/ministry-of-defence/about/procurement#invoice-processing

12. Forms and Documentation are available through *:
Ministry of Defence, Forms and Pubs Commodity Management
PO Box 2, Building C16, C Site
Lower Arncott
Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)

	Applications via fax or email: DESLCSLS-OpsFormsandPubs@mod.uk
7. Quality Assurance Representative: Commercial staff are reminded that all Quality Assurance requirements should be listed under the General Contract Conditions. **AQAPS** and **DEF STANs** are available from UK Defence Standardization, for access to the documents and details of the helpdesk visit http://dstan.uwh.diif.r.mil.uk/ [intranet] or https://www.dstan.mod.uk/ [extranet, registration needed].	***NOTE** 1.Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site: https://www.aof.mod.uk/aofcontent/tactical/toolkit/index.htm 2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

Schedule 5 - Contractor's Commercially Sensitive Information Form (i.a.w. condition 13) for Contract No: CCDT/491

Contract No: CCDT/491
Description of Contractor's Commercially Sensitive Information: All references to pricing information
Cross Reference(s) to location of sensitive information: Annex A to Schedule 2 – Pricing of the Statement of Requirements
Explanation of Sensitivity: The information comprises commercially sensitive pricing.
Details of potential harm resulting from disclosure: Adverse financial impact of a reduction in competitive advantage in the marketplace
Period of Confidence (if applicable): Perpetual
Contract Details for Transparency / Freedom of Information matters: Name: ANTHONY HARRIS Position: COMMERCIAL DIRECTOR Address: Telecom House, 125-135 Preston Road, Brighton, East Sussex, BN1 6 AF Telephone Number: 0845 677 4480 Email Address: tharris@tlmnexus.com

Schedule 6 - Hazardous Contractor Deliverables, Materials or Substances Supplied under the Contract: Data Requirements for Contract No: CCDT/491

Not Applicable

Schedule 7 - Timber and Wood- Derived Products Supplied under the Contract: Data Requirements for Contract No: CCDT/491

Not Applicable

Schedule 8 - Implementation Plan

[Redacted]

Annex A to Schedule 8 - Data Migration Plan

1 Introduction

The Contractor has a comprehensive data migration process for importing historical and archived records, entities and artefacts, maintaining relationships between data elements.

2 Key Activities

A programme plan for Data Migration is shown at the end of this Annex A to Schedule 8. Detailed below are the related Key Activities.

2.1 Data Analysis

Firstly the Contractor shall analyse and confirm the structure, format and content of the data in order to produce data mapping documentation, which includes mandatory / non-mandatory fields and explains the relationship between data elements, entities and artefacts. The documentation also captures current workflow status for open records, as well as any user access requirements. During this phase the Contractor may require access to an Authority representative with extensive knowledge of the data. This will ensure a quick resolution to any impediments, such as missing data for mandatory fields.

2.2 Data Preparation

The Contractor has developed a series of data migration templates, which includes cross-mapping information resident within RESOLVE V1 to the proposed target environment (RESOLVE V2). Wherever possible, when migrating data from outside RESOLVE, the Contractor requests that data shall be presented to the Contractor using these templates, to ensure amore efficient and reliable data migration process, whilst also preventing the loss or corruption of any data.

2.3 Testing and Validation

The verification of data by the Contractor shall consist of a number of discrete checks, which includes cross checking the number of records, entities/issues, artefacts and number of users between the source and destination database. Sample and dip checks are conducted by the Contractor for each and every entity type, including links to other entities and artefacts. A series of printed versus on-screen checks are also carried out. Integrity, Availability and Authenticity checks are also performed by the Contractor for each and every entity type. A full audit trail shall be maintained by the Contractor for all data verification activity within the Contractor’s bespoke verification dashboards.

2.4 Go-Live

The Contractor’s migration process has 16 independent quality gates and the final quality gate requires a go / no-go meeting to be held with the Contractor’s Service Management Team, where a final review is performed to ensure all go-live criteria has been met. Providing all the necessary criteria has been met, written go-live

authority is provided by the Service Management Team and the data is released, in line with the data migration plan. The relevant area of RESOLVE V2 will be temporarily taken off-line whilst the live release is performed. This is arranged in advance with the Authority and it ensures no data is added or modified during the live data migration process.

3 Implementation Risks and Proposed Mitigations

3.1 Risk 1: Loss or corruption of provided data during the data migration process. May delay Go-Live.

Proposed mitigation:

- The data is required to be provided to the Contractor in the correct format using the Contractor provided data migration templates.
- the Contractor shall comply with their data migration process and conduct robust data integrity verification.

Fall Back Plan (include if risk realisation would prevent Go-Live): Back up copy taken of data pre-Go Live. If data loss/corruption then execute data roll-back / restore activity and then re-run migration activity.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive. Additionally, existence of back up copy and roll back capability provides for an achievable fall back solution if required (subject to Authority agreement).

3.2 Risk 2: Loss of network connectivity during live data migration.

Proposed mitigation:

- the Contractor take back up copy of data pre-go live.
- the Contractor execute data roll-back / restore activity and then re-run migration activity.

Fall Back Plan (include if risk realisation would prevent Go-Live: NA.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

3.3 Risk 3: Unexpected and unplanned changes to the data structure and data content during the migration phase.

Proposed mitigation:

- Data format to be migrated is required to remain in a stable structure from Contract Start. The Authority is required to support an agreed data snapshot date prior to final migration no later than 10 Working Days before the Go-Live date.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall

configure the system incrementally using MoSCoW principles at Appendix A to Schedule 8 based on the impact to the go live date.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Data Migration Plan - [Redacted]

Annex B to Schedule 8 – Software Configuration Plan

1 Introduction

RESOLVE V2 is a single code base, supported by a consistent logical database structure, including consistent naming conventions. All the required configuration is maintained within the DES AIMS database. This is managed internally by suitably qualified and experienced Contractor personnel using the Contractor's configuration tools.

2 Key Activities

A programme plan for Configuration is shown at the end of this Annex B to Schedule 8. Detailed below are the related Key activities.

2.1 Configuration Analysis

The implementation phase commences with an analysis of the change, which produces low-level requirements for configuration. This may include data dictionaries, class diagrams, process flows, data mapping, domain model, stakeholder management, user access mapping, role capability mapping, functional / non-functional requirements and User journey. We have these artefacts for the current RESOLVE V1 deployed for the eight remaining Air Systems and can therefore compare these straightforwardly to the new RESOLVE V2 target system. Thus saving time and effort and reducing the dependency upon the Authority.

2.2 Realisation of Software Configuration

Once the analysis is complete and artefacts have been reviewed and approved by the Contractor's change approvals board, the Contractor's development team starts the process of configuring the software. This begins by creating a new baseline under version control from the Contractor's existing Configuration Management Data Base (CMDB). Following a successful peer review, the up-versioned configuration is then extracted using the the Contractor's configuration tool to prepare and deploy the changes to the Contractor's dedicated and secure test environments for all applicable air systems

2.3 Configuration Testing

The Contractor's test strategy sets out the scope and levels of testing required for each group of configuration changes. The strategy takes into consideration complexity, performance, dependencies, levels of user access and data migration needs. Using the analysis artefacts, a full and comprehensive suite of test cases are produced, managed and recorded by the Contractor's highly skilled team of software testers using the Zephyr software test management tool. The Contractor's team uses a combination of unit, manual and automation testing to cover over 8,000 test cases used for the 18 Air Systems rolled-out so far.

3 Implementation Risks and Proposed Mitigations

Risk 1: Failure by Authority to provide agreed process flows.

Proposed mitigation:

- The data is required to be provided to the Contractor in the correct format using the Contractor's provided configuration templates.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall revert to process flows currently in use by the Dts.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Risk 2: Failure by Authority to provide eCassandra Hazards data.

Proposed mitigation:

- The data is required to be provided to the Contractor in the correct format using the Contractor's provided configuration templates.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall configure the Hazard Log in the format in use by the DT currently in RESOLVE V1.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Risk 3: Failure by Authority to provide User account details in order to establish Authorised Users.

Proposed mitigation:

- The data is required to be provided to the Contractor in the correct format using the Contractor's provided configuration templates.

Fall Back Plan (include if risk realisation would prevent Go-Liv): the Contractor shall configure the system for a limited number of users in use by the DT currently in their copy of RESOLVE V1 based on MoSCoW (See Annex A)

Risk Level: Considered LOW as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Risk 4: Extant or supplied process flows are modified by the Authority during the implementation phase.

Proposed mitigation:

- Moratorium on process flow changes from 15 April to Go Live date.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall configure the system incrementally using MoSCoW principles (see Annex A) based

on the impact to the go live date.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Risk 5: Extant or supplied entities are modified by the Authority during the implementation phase.

Proposed mitigation:

- Moratorium on entity changes from 15 April to Go Live date.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall configure the system incrementally using MoSCoW principles (see Annex A) based on the impact to the go live date.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Risk 6: Additional and unexpected configuration to reporting is required by the Authority during the implementation phase.

Proposed mitigation:

- Moratorium on report configuration from 01 April 19 to Go Live date.

Fall Back Plan (include if risk realisation would prevent Go-Live): the Contractor shall configure the system incrementally using MoSCoW principles (see appendix A to Schedule 8) based on the impact to the go live date.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive.

Software Configuration Plan – [Redacted]

Annex C to Schedule 8 – Software and Network Approval Plan

1 Introduction

Software and Network Approval requires that the DES AIMS is fully accredited and gains authority to operate on the Assured LAN Interconnect (ALI). The Contractor shall ensure that all parts of JSP604 are met along with DEF STAN 05-138, and that DES AIMS represents the latest Industry best practices. In addition, the requirement to adhere to DEFSTAN 00-56 Safety Management Requirements for Defence Systems means that DES AIMS is to be considered a Product, Service and/or System (PSS) and must meet the requirements in terms of safety management, engineering for in-service.

2 Key Activities

A programme plan for Software and Network Approval is shown at the end of this Annex C to sSchedule 8. Detailed below are the related Key activities.

2.1 Achieving DES AIMS Accreditation

Upon receipt of the Cyber Risk Profile from the Authority the Contractor shall complete the Supplier Assurance Questionnaire (SAQ) on Octavian. The Contractor shall then prepare the Risk Management Accreditation Document Set (RMADS) that clearly demonstrates the required compliance with, JSP604 – Network Joining Rules, DEFSTAN 05-138 and ISO27001/2 principles. The Contractor's RMADS will then be uploaded to the Defence Assurance Risk Tool (DART). The Authority will then assess, query and/or grant approval to operate. During this process the Contractor shall continue to be a certified Cyber Essentials & Cyber Essentials Plus Organisation, we will engage with an approved assessment body to carry out the on-site assessment, prior to Go-Live.2.2 Provide DES AIMS Safety Case Report

The Contractor shall engage with Authority Safety Representative to agree provision of required safety artefacts in accordance with Contractor requirements shown in DEFSTAN 00-56 Safety Management Requirements for Defence Systems. Artefacts can include Hazard Analysis and Safety Case Reports.

4 Implementation Risks and Proposed Mitigations

Risk: The MOD is not able to progress submitted accreditation documentation during Implementation phase due to other priorities. This may result in accreditation approval not being provided by the Go-Live date.

Proposed Mitigations:

The Contractor shall provide submission early in implementation phase to allow for maximum opportunity to resource approvals.

tlmNexus provides comprehensive submission (requiring reduced Authority effort to approve.

tlmNexus/Authority submission requiring limited Authority effort to approve.

Authority representatives to liaise with Assigned Accreditor early over submission timings and approval tasking.

Fall Back Plan (include if risk realisation would prevent Go-Live): If no accreditation of DES AIMS received by Go-Live then Authority would be requested to permit continued use of the existing RESOLVE tool for a short period until DES AIMS is accredited.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive. Additionally, existence of existing tool provides for a feasible fall back solution if required (subject to Authority agreement)

Risk: The MOD make fundamental changes to the accreditation process and associated processes (e.g JSP604) during the implementation phase and before accreditation has been provided. This may result in accreditation approval not being provided by the Go-Live date.

Proposed Mitigations:

The Contractor shall provide submission early in implementation phase to allow for maximum opportunity to achieve approval before process change.

Authority DES AIMS representatives to liaise with Assigned Accreditor early over submission timings and confirm likelihood of changes to process.

Fall Back Plan (include if risk realisation would prevent Go-Live): If no accreditation of DES AIMS received by Go-Live then Authority would be requested to permit continued use of the existing RESOLVE tool for a short period until DES AIMS is accredited.

Risk Level: Considered low as proposed mitigations to prevent realisation are considered sufficiently layered and comprehensive. Additionally, existence of existing tool provides for a feasible fall back solution if required (subject to Authority agreement)

Software and Network Approval Plan – [Redacted]

Appendix A to Schedule 8 – MoSCoW Definition to be used in a Fall Back scenario

In the Risk mitigations above particularly in Data Migration and Configuration the Contractor has defined a fall back position based on MoSCoW. The table below will assist the Contractor and Authority to define fall back options in that eventuality

	MUST have this requirement to meet the business needs	**SHOULD have requirement if at all possible, but the project success does not completely rely on this**	**COULD have this requirement but it does not affect the fitness of business needs of the project.**	**WON'T have this time but WOULD like in the future. Alternatively WANT**
	Minimum **U**seable **S**ubse**T** If even one MUST requirement is not included, the project delivery should be considered a failure	Significant benefits, but not necessary for delivery in the current delivery time-box. <SHOULD> requirements are often not as time-critical or have workarounds	Significant benefits. Work-Around is easy or cheap. Requirements labelled as <COULD> are less critical and often seen as *nice to have*	Out of Scope this time
the Contractor …	*…will absolutely guarantee this*	*…will go all out to achieve this*	*…will give it their best endeavours, but no guarantee*	*…will re-prioritise next time, in the next release.*
	60% of the effort	40% of the effort		0% of the effort

Previous similar transitions have been successfully implemented through an agreed use of the Initial and Final Operational Capability (IOC and FOC) method. If for any reason the timescales are under threat and a Fall Back scenario is required a combination of MoSCoW, IOC and FOC will be negotiated and agreed with the Authority via an Authority SPOC to co-ordinate these decisions to DE&S on behalf of the programme as a whole in this fall back scenario.

Typically the working relationship between MoSCoW and FOC, IOC in the event of any slippage is as follows.

IOC	FOC
MUST	COULD
SHOULD	WOULD

Schedule 9 – Training Plan

1 Introduction

Delivering effective training in a consistent and convenient manner is fundamental to the successful use of RESOLVE, an off-the-shelf software solution provided to meet DES AIMS requirements. To enable this, the Contractor employs a training team, including fully qualified trainers who are experienced in the user community, Military Aviation and have a comprehensive understanding of RESOLVE. The trainers are responsible for tailoring, designing, updating, scheduling and delivery of the training. This will be coupled with our integrated training booking service through our DES AIMS Online Support Facility, as well as users having access to a host of user guides and online training modules via RESOLVE itself.

This Training Plan is the product of having completed a detailed Training Needs Analysis (TNA) for the related software, its planned use and the user community involved. The TNA identified the need to include a wide variety of training methods, as well some very specific approaches to our delivery. Additionally, we understand the need to include innovation and flexibility in our solution in order to cater for supporting those people working within a Military Aviation Environment.

2 Training Methods

The proposed solution is almost entirely based on the existing Resolve software provided to DE&S so the current 6,300 Authorised Users are already competent with the software. The TNA ensures the training needs of the Authorised Users have correctly been identified and are able to access a variety of training methods specifically designed and tailored to ensure they are competent to operate DES AIMS and as such can manage Events, Issues and Entities effectively and efficiently without supervision. These range from using the Contractor's online modules, through to delegates using our interactive training suite to work real world scenarios in a structured and controlled environment.

2.1 Online Training

Online Training will be made available for the Authorised Users using a variety of modules which are fully structured and linked. These will include syllabuses that can cater for a complete overview of the tool, through to more detailed instructions on how to work through one of the AIMS processes. The Contractor's online modules provide a common and familiar user experience and are provided in accordance with UK Government Assisted Digital Guidance and accredited where required within the Government Digital by Default Services Standard. They will predominantly be available through the DES AIMS and users will be able to access the Online Training as soon as they have an Authorised User account. Online training modules will be developed and tested in accordance with the Application Development Framework.

2.1.1 SCORM Compliance All online training content is designed and configured to be compliant with the Shareable Content Object Reference Model (SCORM), thus allowing for the Authority in the future (where appropriate) to host and utilise these

training modules themselves for the purpose of training Authorised Users in DES AIMS.

2.2 Integrated User Guides

Integrated user guides are provided for the four Authorised Users Types including those with the System Administration role. These are accessed from the Help Centre in DES AIMS and cover the more generic functionality in the tool such as editing a form. An example of the type of guide available is at Figure 1. For more specific information on the application of a process, a wide variety of process guides are maintained in the 'Common Documents' area in DES AIMS. These provide much more content, giving a step by step guide (including a number of screenshots) for the user to print out and have on their desk whilst working through a particular process.

[Redacted]

2.3 On Screen Prompts

DES AIMS comes with a variety of on screen prompts to assist the Authorised User in a wide range of situations. For example, detailed prompts will appear to the User when they try to enter incorrect data or when they try to advance the process to the next step without having entered all the mandatory data. This is achieved within the software by the Manual Update Trigger (MUT) rules configured appropriately for each process. The MUT rules guide the Authorised User down the approved path and makes DES AIMS both rigorous in terms of correct process completion, but also highly intuitive to use which improves user behaviour, output whilst reducing the training burden. It is worth highlighting that DES AIMS includes additional capability to tailor user options depending previous selection. For example, this ensures only appropriate reference data entries are made available that conform to a Part Number nomenclature.

2.4 Instructor Led Training

The Contractor's dedicated training team allows the Contractor to make maximum use of Instructor Led training for the users through a variety of options from Face to Face (F2F) to Webinar training. Such training requires increased commitment in terms of time and resources for both parties. However, it is appropriate to use this approach in certain circumstances, when principally supporting a highly regulated environment that manages complex airworthiness and safety process and procedures.

2.4.1 Face to Face (F2F) Training

F2F training is provided in two distinct formats; interactive and demonstration. The format used will be a decision usually based on the training content, with each having its own advantages.

2.4.1.1 Interactive Training.

Interactive training allows delegates access to a 'sandpit' copy of DES AIMS that

fully replicates the functionality available to the Authorised User at that time. This method is facilitated using a mobile Interactive Training Suite (ITS), which provides IT hardware (e.g. linked and integrated laptops) for up to 10 delegates to work in the same room.

During the interactive training sessions, highly skilled trainers walk the delegates through real world MAE practical scenarios and allow each of the delegates to enter and manipulate data, understand process flows and save data and operate the tool in the correct manner. This ensures the delegates develop the relevant system understanding required as part of their job/role. Printed workbooks are provided and the duration of the training session is planned to be no more than three hours.

The trainers require pre and post course access to configure the customer-provided training facility in preparation for the training sessions and to leave the facility in the condition it was received. Provision of this type of training requires a significant commitment by both parties and so there is a minimum requirement of five confirmed delegates for each course.

2.4.1.2 Demonstration Training.

Demonstration training is predominately used for large groups of delegates and can include generic overviews of the tool as well as specific training on a particular process. Each demonstration session begins with a PowerPoint presentation, which is followed by a series of trainer led on-screen demonstrations of the tool. Printed workbooks provide guidance notes for delegates with the duration of the training session no more than two and a half hours including 30 minutes for Q&A. This type of training can be scaled, with a maximum of 20 delegates per session, with a minimum confirmed attendance of five.

2.4.2 Telephone Training

Telephone training can be offered to Authorised Users who are unable to travel to a F2F training location. A session time is booked and a link to the training material is provided or the material emailed to the delegate. During the training session the trainer will provide one-on-one guidance and instructions over the phone. For this training it is recommended that delegates have access to a telephone headset. The training duration depends on the tailored content (no more than 60 minutes), but this type of training has its limitations and would be used by exception only; for example, to meet urgent operational needs.

2.4.3 Webinar Training

Subject to both parties being able to communicate using Skype for Business, then Webinar training is available. For example, this can be made available for Authorised Users who may require a short demonstration in one or two key system functions. This method will need to include screen sharing to allow the delegates to view the trainer’s screen whilst listening to the live instruction.

A Skype invitation is sent to one or more Authorised User and at the appointed time the webinar is delivered. The Skype webinar training duration depends on the required content, but these sessions are normally brief, lasting no more than 60

minutes. A pre-prepared synopsis of the training is sent out in advance of the session by email, which can also provide a useful guide for further application of the skills and knowledge gained in the session.

2.4.4 Delegate Feedback

Delegates complete feedback forms after all courses, identifying what they thought of the course content and the ability of the trainer. This information is vital to help maintain the highest standards of delivery and for the DES AIMS contract feedback will be shared with the Authority to highlight any improvement actions we are taking.

3 Approaches to DES AIMS Training

The approach to training has been divided into three distinct classes to accommodate the various needs of the contract and the Authorised Users. In each class the approach and training content is tailored to maximise the impact of the training whilst minimising any disruption to the Authority, their daily commitments and business environment during delivery. These approaches are explained in detail within this section and Figure 2 below highlights the training summary for delivery before Go-Live.

[Redacted]

3.1 User Readiness Training

User Readiness training requires that that all 6,300 Authorised Users have sufficient awareness and/or training to enable them to access and use the DES AIMS. The contract requires that a minimum of 25% of Authorised Users shall be trained to operate the system competently by Go-Live, with the remainder given sufficient awareness and/or training to enable them to access and use DES AIMS by the Authority to Operate (AtO) date. As the DES AIMS solution is almost entirely based on the existing RESOLVE, Airworthiness Information Management, software provided to DE&S, then the existing 6,300 Authorised users are already competent with the software and thus the User Readiness Training burden and associated risks are extremely low.

3.1.1 Data Migration Training

As identified in the Data Migration Plan (Annex A to Schedule 8) it will be necessary for the Authorised Users working with 8 of the 26 Air Systems to be moved from their current version of Resolve to the latest version of Resolve in order to align with the required DES AIMS solution and the Authority's 'Data Migration Vision for the Future'. When this happens the Authorised Users will need simple awareness training on the additional features provided, including some minor changes to the user interface. This migration will take place before Go-Live and will be dealt through a combination of Online Migration Training modules made available to all and also F2F demonstration training provided for key nominated personnel.

For each Air System the awareness training package provided will need to be adjusted to cope with the organisational differences within the related Delivery Teams (DT). The training package will be formulated in agreement with each DT to

ensure full and proper coverage and will include tailoring of the course content as required. This migration activity is very familiar to the Contractor and excellent results have been achieved with our training delivery in these circumstances, reducing disruption to a minimum whilst also using the training opportunity to promote more effective and greater use of the tool.

3.1.2 DES AIMS Alignment Training

For those Authorised Users who are not involved in the Data Migration Training, alignment training will be available to provide awareness of the additional features included in DES AIMS after Go-Live. To deal with this a very specific Online Alignment Training module will be made available to all Authorised Users at least four weeks before Go-Live. Whilst we could provide this module earlier, experience suggests that completing the course early would potentially lead to unnecessary skills-fade before Go-Live negating the training effort. The module will take no more than 20 minutes to complete and will ensure all Users who are already competent with using the existing solution, are fully informed of how to take advantage of all the additional functionality. There will be no limitation to the number of users able to access the course at any time and with the Authority's assistance, we will be advertising the course using various means well before Go-Live. This will ensure everyone understands the needs and benefits of spending this short time being trained and promote maximum take up.

4 New User Training

New User Training will be provided throughout the term of the contract after Go-Live to enable all new users to operate the DES AIMS competently. The Authority will determine who they would include within this training, but we would expect a new user to be someone who has not used the tool before or returning as an Authorised User after a break in use. Additionally, new users can be delegates that need to adopt a new DES AIMS role such as the System Administrator or even those who need to change their User Type (as defined in the Authority's 20181022 DES AIMS Access Strategy). The Authority is encouraged to mandate training of this nature to all its new users and all new users would benefit most from F2F training. Provision for this has been made, with capacity for up to 1500 course places provided per annum (Apr – Mar). A typical training syllabus for this F2F training is as follows:

- Accessing the tool
- Originate, process, track and record Issues and / or Entities
- Assign and reassign Issues and / or Entities to another User
- Assign Actions to other Users
- Record any decision of review, amendment or approval
- Provide comments and / or justification for approvals / decisions
- Understand the implications of mandated fields
- Close or archive an Issue and / or Entity
- Search the DES AIMS for Issues, Entities, Artefacts and Actions
- Recover details of Issues and / or Entities
- Print content from within DES AIMS
- Export content from within DES AIMS

- Import content into the DES AIMS
- View and make comments on digital Artefacts attached to Issues and / or Entities
- Access audit trail of decisions and evidence underpinning the progression of an Issue
- Re-open a closed or archived Issue and / or Entity
- Linking Issues/Entities and Artefacts
- Attach digital Artefacts to Issues and / or Entities
- View a summary of all Actions assigned to them, including deadlines and priorities
- Manage assigned items

As the new user is provided with their account they will be emailed a welcome message providing instructions for links to the DES AIMS Online Support Facility. From here the new user will be able to request their preferred locations for the training, as well as a suitable time frame for completion. Each week the Training Team will consolidate the requests and identify the best sites and dates for the F2F training to accommodate the needs of the delegates, noting that as many as 180 delegates per month can be accommodated. Where the user will not be able to attend a F2F training session (e.g. for operational reasons), alternative methods of Instructor Led training such as provision of a Webinar will be available.

In addition the F2F training, when the new user first accesses DES AIMS they will be able to use a short Introduction Online Training Module. This is specifically designed to meet their immediate needs for using the tool and completing basic functions, thus avoiding the need for the new users to seek advice from colleagues.

5 Top Up Training

Top Up training for Authorised Users will be needed where changes have been made to the DES AIMS, introducing new features and/or services. The decision on which training method will be used to support the new feature/service will be made during the design/development phase of the new feature/service and this will be shared/agreed with the Authority. In each instance a combination of training types will be selected to best match the complexity and coverage of the new feature/service being introduced.

An example of the application of Top Up training would include where the DE&S Airworthiness Team (DAT) issue a new policy instruction. This would necessitate a change to the DES AIMS functionality in order to align an existing process to new or amended Military Aviation Authority (MAA) Regulation. If this happens then users who are familiar with the existing related process may need to be additionally trained in the inclusion of new data fields or workflow steps. In this situation a short Online Top Up Training Module is made available to all Authorised Users. An example of an online training slide is shown in Figure 3. At the same time F2F training would be made available for those users within the DT closely associated to the management of the process being changed. This training will be scheduled to complete before release of the new functionality, but resources can be made available to assist those after release, who may have been unable to take up the training opportunities due to other commitments. This approach ensures appropriate knowledge transfer/skill gain

with the minimum disruption to the Authority.

[Redacted]

6 Provision of Training Facilities

The preferred location for F2F training is the dedicated training facility at the Contractor's office in Brighton; however training will also take place at main Authority sites in order to reduce Authority travel costs and user time spent away from the workplace. Trainers will travel to the main Authority sites in the UK during the contract in order to deliver the training. The Authority will be required to provide the appropriate facilities to ensure the right environment is available for learning. For F2F training this would be a meeting room facility, including tables/chairs for all delegates and a screen and projector to connect to the trainer's laptop.

F2F Training can also be provided overseas as agreed on a case-by-case basis as an Additional Service under Schedule 13 – Additional Tasking Service.

6.1 Room Booking & Access

Where F2F training is to take place on a main Authority site, the Authority will need to appoint a local point of contact who will coordinate the booking of rooms, facilities and access to the site/building for the trainer(s) (and Authorised Users where necessary). Proposed dates for the training will be agreed with the local coordinator based on the training requests received. Once a room booking is made the actual training date will be confirmed to the Authority. The local co-ordinator will be responsible for ensuring all delegates are advised of the training location/date/time and any specific access arrangements they may require.

6.2 Attendance

The training date will be chosen to enable the maximum number of delegates to attend. However, after making the room booking the delegate number may change for various reasons including operational commitments down to a minimum level, after which the course will be cancelled. Minimum attendance levels for the course are identified in Section 2 (Training Methods). 10 days notice of cancellation is required; where cancellation happens after this point, or if fewer than the minimum number of delegates actually attend, the course will be classified as delivered to the minimum number of delegates. This number of delegate places will be deducted from the annual target for F2F training. This does not prevent the users themselves booking onto future courses.

Training Plan – [Redacted]

Schedule 10 – Exit Strategy

1. Introduction

1.1 The Exit Strategy facilitates the smooth transition of DES AIMS to a new service provider or the Authority with minimum disruption as well as preventing or mitigating any inconvenience to the Authority. The Exit Plan shall set out the steps to be followed on the termination (including Partial Termination) or expiry of this Contract. The Exit Plan shall support an orderly, controlled transition of responsibility for the provision of the Contractor Deliverables from the Contractor to a new service provider or the Authority. The Exit Plan that shall apply is provided at Annex A to this Schedule.

2. Exit Objectives

2.1 The following exit objectives hereunder shall be addressed in the Exit Plan:

a. Transition – the Exit Plan shall detail how the Contractor will cease to supply the Contractor Deliverables, or part thereof, and enable a new service provider or the Authority to perform equivalent (or similar) services. This shall include clear steps and working practices that avoid barriers or restrictions that together enable a smooth transition of DES AIMS. The Exit Plan shall also address how any negative impact, including disruption or deterioration of DES AIMS service shall be managed;

b. Assistance – the Exit Plan shall detail the assistance and information that the Contractor shall provide to a new service provider or the Authority to achieve an efficient and effective transfer of DES AIMS. This shall include how the Contractor shall work with a new service provider and / or the Authority to plan, manage and execute the DES AIMS transition;

c. Data migration – the Exit Plan shall set out how the Contractor will provide all stored Data and attachments in an open source data format, preferably a SQL Server database format. It should also provide an explanation of how the relevant connections between tables/data entities logical data structure) will be maintained to enable the data to be migrated;

d. Data transfer – the Exit Plan shall set out how the Contractor will ensure that Data is not compromised during the exit process.

3. Review of Exit Plan

3.1 The Contractor shall (at no cost to the Authority), on a six (6) monthly basis starting at the commencement of this Contract and at any other time the Authority or the Contractor deems necessary throughout the Term:

a. review and revise the Exit Plan to take into account changing technologies or required amendments by the Authority and any changes to the scope or nature of the DES AIMS services;

b. inform the Authority of the outcome of any review of the Exit Plan and identify any necessary updates; and
c. agree with the Authority the scope and detail of any necessary revisions to the Exit Plan and shall promptly and in any event within ten (10) Working Days submit such revised Exit Plan to the Authority for approval.

3.2 Without limitation to the generality of the foregoing, the Contractor shall promptly make such amendments to the Exit Plan as the Authority may reasonably require from time to time.

4. Disclosure of Exit Plan

4.1 The Contractor agrees that, notwithstanding any of the Authority's obligations of confidentiality under this Contract, the Authority may at any time disclose the Exit Plan and/or any documentation to a new service provider who are tendering or involved in the tendering process to take over provision of the Contractor Deliverables or substantially similar services on termination, Partial Termination or expiry of this Contract.

Annex A to Schedule 10 – Exit Plan

1 Introduction

The Exit Plan sets out the steps to be followed to enable an orderly and controlled transition of responsibility for DES AIMS to a new service provider or the Authority on the termination (including Partial Termination) or expiry of the Contract. As described below the factor that will mitigate and ensure an orderly transition for both parties is to maximise the notice period available.

2 Exit Plan Aim & Scope

The aim of this Exit Plan is to allow for any of the exit scenarios described to be completed with minimal disruption and inconvenience to the Authority and DES AIMS. It achieves this by addressing each of the exit objectives in detail for Transition, Assistance, Data Migration and Data Transfer, as identified in the Authority's Exit Strategy. This Exit Plan considers the following exit scenarios:

- **Partial Termination.** Partial Termination of the Contract and as such part transition of the data within DES AIMS to the Authority or (subject to paragraph 6) a new service provider. This could include, but is not limited to:
    - Removal or cessation of one or more Air Systems or Delivery Teams (DT) from DES AIMS.
    - Removal or cessation of use of one or more entire processes from DES AIMS. This may be for all or part of the Authorised User community.

- **Full Termination.** Full termination or expiry of the Contract and transition of all Data to the Authority or (subject to paragraph 6) a new service provider.

- **Test Data Load**. Testing and verification of the viability of the Exit Plan throughout the Term of the Contract. This tasking is primarily focussed on a scenario where the Authority wishes to test the Exit Plan and its drills without the actual intent to terminate (in whole or part). We recommend that these test data loads coincide with the review and therefore are coincident with the review and happen every six months as a maximum.

3 Transition

The Notice period for terminating the Contract shall be twenty (20) days. Notwithstanding the termination periods given in the Contract and the notice periods stated in the Authority's future vision for data migration[1], the Contractor acknowledges that the best possible notice periods are needed from the Authority to support transition. This is in order to mitigate the inherent risks associated with this activity, and to enable the Authority's requirement in its Exit Strategy for a smooth transition with minimum disruption as well as preventing or mitigating any inconvenience to the Authority. The Authority may extend the Notice period for terminating the Contract. Any decision to extend the Notice period is a matter solely for the Authority and the

[1] Authority's ITT document: 201181022 DES AIMS Data Migration Future Vision

Authority's decision in this matter will be final.

3.1 Partial Termination

The Authority shall use reasonable endeavours to provide the Contractor with 45 days' written notice for Partial Termination of the Contract in order to facilitate the most orderly and controlled transition of DES AIMS. Upon giving notice, the Authority will need to define the Termination Date (TD) for the Terminated Service and the Stop Access Date (SAD) for the DES AIMS. The SAD is the date after which no further changes are made to the Data through the restriction of Authorised User access to DES AIMS. In this situation, the following two options will be available:

1. Suspension of Terminated Service. The SAD is 10 or more working days prior to the TD in order to ensure the data is stable and the data subsequently transferred has not been modified.

2. Continuation of Terminated Service. A continuation of use of the Terminated Service until TD (i.e. SAD=TD), noting that the Data when subsequently transferred could be up to 10 working days out of date.

3.1.1 Data Sets Provided

3.1.1.1 Sample Data Set

The Exit Plan will be executed firstly by way of production of a Sample Data Set (SDS) of not more than 1000 data records from DES AIMS. This SDS will be delivered to the Authority 10 working days after notice is given by the Authority for Partial Termination of DES AIMS.

3.1.1.2 Final Full Data Set

The Final Full Data Set which will comprise all Data records within DES AIMS will be provided to the Authority 10 working days after the SAD or the TD, whichever is the earlier.

3.2 Full Termination

The Authority shall use reasonable endeavours to provide the Contractor with 90 days' written notice for full termination of the contract in order to facilitate the most orderly and controlled transition of DES AIMS to the Authority or a new service provider. Upon giving notice, the Authority will need to define the TD and the SAD for DES AIMS. In this situation, the following two options will be available:

1. Suspension of Terminated Service. The SAD is 10 or more working days prior to the TD in order to ensure the data is stable and the data subsequently transferred has not been modified.

2. Continuation of Terminated Service. A continuation of DES AIMS until TD (i.e. SAD=TD), noting that the data when subsequently transferred could be up to 10 working days out of date.

3.2.1 Data Sets Provided

3.2.1.1 Sample Data Set

The Exit Plan will be executed firstly by way of production of a Sample Data Set (as defined in above). This Sample Data Set will be delivered to the Authority within 10 working days after the notice is given by the Authority for Full Termination of the Contract.

3.2.1.2 Trial Full Data Set:

At a time to be agreed by the parties, but not less than 10 working days after the SDS is provided, the Contractor will provide a Full Data Set as a trial to the Authority to allow the Authority or, under the Authority's supervision, the new service provider, to conduct volumetric testing and assurance activity.

3.2.1.3 Final Full Data Set

The Final Full Data Set will be provided to the Authority within 10 working days after the SAD or the TD, whichever is the earlier.

It should be noted that as described only two full priming loads (Trial Full Data Set and Final Full Data Set) will be produced by the Contractor to support Full Termination. Not only are these priming loads potentially time consuming to produce, but they may reduce the quality and availability of the extant service as services may need to be taken offline to produce the load (by agreement with the Authority). Any additional priming loads needed by the Authority to support Full Termination will need to be contracted for in accordance with Schedule 13 – Additional Tasking Service.

3.3 Test Data Load

The Contractor requires 10 working days' notice from the Authority to provide a whole or sample catalogue of the data to the Authority. DES AIMS will not be suspended during the production of such catalogues. This will be a test run and as such the Authority agrees that no more than one test will be run per six months during the term of the Contract.

3.3.1 Test Data Set

Within ten working days after notice is given by the Authority, the Contractor will provide a single, full or part snapshot of the data to the Authority. As the data will be continually changing, the data could be up to 10 working days old by the time it is delivered to the Authority.

4 Assistance

The level of assistance from the Contractor to allow a successful transition will depend upon the nature of the target system and knowledgeability of the new service provider. the Contractor will provide the following key artefacts to ensure disruption is minimised and mitigate inconvenience to the Authority. They include:

- A populated copy of the AIMS Exit DB described below.
- Comprehensive test results verifying the AIMS Exit DB data extract.
- Technical documentation describing the AIMS Exit DB for use in the transfer of data assets.

Subject matter expertise shall be provided by the Contractor knowledgeable in the following key aspects of the data migration but not limited to:

- Data Architect expertise
- Information security expertise
- Data migration expertise

4.1 Standard Assistance

Standard Assistance covers Subject Matter Expert support by the Contractor to the Authority and/or new service provider supporting technical questions regarding the technical documentation and Data provided as part of the Exit Plan. Standard Assistance includes:

- Documented answers to technical questions as a result of the deliverables listed above. Effort not to exceed two man-days within the notice period. The Contactor recommends that these formal questions are supplied in a standard format and responses tracked against target response dates.
- The Contractor shall attend up to two collaboration meetings hosted and chaired by the Authority at Abbey Wood within the notice period.

Where more Standard Assistance is required by the Authority, then additional support can be agreed with the Authority and contracted in accordance with Schedule 13 – Additional Tasking Service.

5 Data Migration

Data migration will follow the following outline process:

- The Data will only include those processes/entities contracted for under DES AIMS and as described within the Contract.
- The Contractor will run a series of SQL queries on the various DES AIMS instances supporting individual Air Systems. This will occur one process and one Air System at a time until all the Data has been harvested.
- During Data harvesting the live application may need to be taken offline with the permission of the Authority, in order not to compromise ongoing operational performance of DES AIMS.
- These extraction queries will be the sole responsibility of the Contractor to execute.

- The Data extraction will be subject to the Contractor's in house verification and peer review.
- A single new database structure (AIMS Export DB) whose sole purpose is the transfer of the data to the Authority will be configured and delivered as part of the Exit Plan.
- The AIMS Export DB will be provided to the Authority and IPR will not apply to this database schema included in this deliverable. The details of this database structure are listed below and represented in Figure 1.

[Redacted]

Figure 1: ERD for AIMS Export DB

[Redacted]

[Redacted]

5.1 Details of the AIMS Export DB

The main purpose of the database is to maintain the logical structure of:

- Issue/Entity links to documents/attachments
- Issue/Entity links to other Issues/Entities
- Issue/Entity Sign Offs

The AIMS Export DB is designed to be as simple and straightforward as possible so as to reduce the time and knowledge transfer required for a new supplier with a basic grasp of database design to understand. By transferring the data to this structure no inherent knowledge of RESOLVE would need to be transferred, the new supplier would need to be familiar with the airworthiness and engineering requirements encapsulated in DES AIMS. Furthermore, the AIMS Export DB will not have to change its structure during the term of the Contract even if the processes and workflows change in order to maintain compliance.

The AIMS Export DB will be accompanied by a technical document providing details of the database structure, content, format and design details. This document will be provided on Contract Award and before the Go Live and reviewed and updated as part of the standard six monthly periodic review.
The simplified data structure is logically consistent and coherent with the requirements and supplies four main tables and two supporting tables:

5.1.1 Main Tables.

- **tbl_Entity** contains a unique ID of every entity from all DTs Resolve instances.
  - It will contain a column to describe the donor Resolve instance e.g. Chinook
  - It will contain a column to describe the Entity Type e.g. SI(T)
  - It will contain XML describing the entity data as a name value pair
- **tbl_EntityJoins** contains a pair of UIDs from the tbl_Entity identifying the link between any two entities
- **tbl_Attachments** contains a UID for every document or attachment
  - It will contain a column for the filename at the time of upload
  - It will contain a column containing the file itself as a binary image
  - It will contain a column containing XML describing some meta data about the file where it exists.
- **tbl_SignOffHistory** contains a Foreign Key relationship to tbl_Entity
  - It will contain XML describing all of the sign offs if any that have occurred against that entity.

5.1.2 Supporting Tables.

- **tbl_ResolveInstance** is a look up of the donor DT referenced by tbl_Entity
- **tbl_EntityType** is a look up of the Entity Type referenced by tbl_Entity

Once the Data is successfully harvested by the Contractor it will be delivered along

with a conformance verification outlining the tests and counts.

6 Data Transfer

The Contractor will only supply the data set in accordance with its obligation to the Authority under the Contract. Transfer of such large volumes of data can present a tangible security risk and it will only be possible to manually transfer the Data on secure removable media. Therefore, to ensure the data is not compromised during the exit process, it is entirely appropriate that the Contractor should only provide the data directly to the Authority. The Authority will then be responsible for making appropriate arrangements for any onward transfer of the data to the new service provider. Figure 2 diagrammatically shows the method for the transfer of the data to the Authority.

[Redacted]

Figure 2: Data Transfer to the Authority

All data transfer will follow the assured Authority procedures for receiving and moving data of this type and volume. This can include secure courier methods and alerting in the event of non-receipt.
The data load will be delivered using removable media in a single SQL Server Back-Up file. Access to the removable media will be supplied separately to avoid inadvertent compromise during transfer.

7 Review of Exit Plan

The Contractor will review the Exit Plan with the Authority once every six months starting at the commencement of the Contract. Reviews will also take place at any other time that either the Authority or the the Contractor deem necessary throughout the Term. The review and any necessary revisions will take into account changing technologies or required amendments by the Authority and any changes to the scope or nature of DES AIMS. The review will also include any updates to the supporting technical documentation describing the detailed information held within the AIMS Exit DB.

On completion of the review, the Contractor will inform the Authority of the outcome and agree with the Authority the revisions needed to the Exit Plan. Once the revisions are agreed by the parties, the the Contractor shall within 10 working days provide a draft revised Exit Plan to the Authority for their approval (such approval not to be unreasonably withheld or delayed). The approved Exit Plan will then supersede all previous Exit Plans once signed and returned by the Authority to the Contractor.

8 Disclosure of Exit Plan

The Contractor recognises that the Authority may at any time disclose this Exit Plan and associated documentation to a new service provider who is tendering or involved in the tendering process to take over provision of DES AIMS or substantially similar services on Full Termination, Partial Termination or expiry of the Contract.

Schedule 11 – Service Levels, Service Level Agreements and Service Credits

Definitions

Service Credits	means service credits being applied to reduce the monthly charge for the DES AIMS service or the DES AIMS system administration service should the Service Level Agreement or system administration SLA not be met
Service Levels	means the level of service provided by the Contractor
Service Level Failure	means a failure to meet the agreed Service Level

Service Level Agreement (SLA) and system administration SLA

The Service Level Agreement (SLA) as per Annex A of this Schedule 11 set out the Service Levels which the Contractor is required to achieve when providing the DES AIMS service in accordance with Schedule 2, the mechanism by which Service Level Failures will be managed and the method by which the Contractor's performance in the provision by it of the DES AIMS services will be monitored. The system administration SLA as per Annex B of this Schedule 11 sets out the Service Levels which the Contractor is required to achieve when providing the DES AIMS system administration service in accordance with Schedule 2, the mechanism by which Service Level Failures will be managed and the method by which the Contractor's performance in the provision by it of the system administration services will be monitored. Failure to meet the Service Levels in either SLA will result in Service Credits to the Authority which shall reduce the monthly charge for the DES AIMS service as per Schedule 2, Table 2 – DES AIMS Service Fee. Service credits shall not be applied until the Go-Live Date has been met.

Service Credits

Service Credits are a reduction of the monthly fee payable in respect of the Contractor Deliverables and do not include VAT. The Contractor shall off-set the value of any service credits against the monthly charge for the DES AIMS service.

Annex A.1 to Schedule 11 – Technical Support

1 Introduction

The DES AIMS Technical Support Service is aligned with the ITIL role separation model for Incident Management, as detailed in Figure 1, which focuses primarily on handling and escalating incidents as they occur. The Contractor's goal is to take user incidents from a reported stage to a satisfactory closed stage, where Problem Management is responsible for finding and removing the root cause of repeated incidents and change management implements the changes necessary to achieve it.

[Redacted]

Figure 1: Levels of Technical Support

The Technical Support Service provides:

- A Service Desk available via telephone, operating between the hours of 7:00 am to 7:00 pm, Monday to Friday (excluding Bank Holidays).
- An online support facility, available on a 24/7 basis.
- A Single Point of Contact (SPOC) through which to access all technical support.
- Technical support, available on a 24/7 basis to resolve incidents, problems and requests.
- ITIL-based support framework and processes.

2 Service Desk

2.1 Operation

The DES AIMS Service provided by the Contractor shall include the provision of a Service Desk capability, operating as the Single Point of Contact (SPOC) for all technical support inputs. The Service Desk will be available to Authorised Users via a dedicated contact telephone number, Monday to Friday (excluding public holidays) between the hours of 7:00 am and 7:00 pm and will be staffed by experienced support personnel with knowledge of the managed service, hosting, airworthiness processes and the key roles involved. The Service Desk will provide 1st Line support to all Incidents, but, depending on the complexity of the Incident, will also conduct certain Second Line support activities, such as data integrity issues. They will also escalate Incidents, Problems and Service Request to 2nd and 3rd Line support. In addition, Authorised Users will be able to contact the Service Desk to obtain information on major outages, interruptions to the Service and planned maintenance down-time.

2.2 Performance

Performance metrics applicable to the provision of the Service Desk are detailed within the Service Level Agreement (SLA) at Annex A.2 to Schedule 11 of SC2.

3 Online Support Facility

An Online Support Facility (OSF) shall be provided by the Contractor, which Authorised Users access from MODNET and approved Industry partner IT systems. The facility will be available continuously and will enable Authorised Users to raise new Incidents and Service Requests and view their status and progression through the life-cycle. Authorised Users will also be able to view information on major outages, interruptions to the Service and planned

maintenance down-time. Incidents reported through the OSF will be acknowledged by the Service Desk and, dependent on the origin and type of the Incident, will be prioritised and then either resolved by the Service Desk or assigned to an appropriate level of support for resolution. Incidents affecting the progression of Entities or Issues within DES AIMS related to Aircraft-on-Ground (AOG) situations will be escalated to 2nd Line support immediately. Visibility of the progression and status of incidents will be provided on the Online Support Facility.

3.1 Performance

Performance metrics applicable to the provision of the OSF are detailed within the SLA at Annex A.2 to Schedule 11 of SC2.

4 SPOC

A Contractor SPOC shall act as the controlling function for all technical support requests. The Service Desk is at the centre of the SPOC, satisfying the ITIL best-practice for Incident Management, where the Service Desk manages the lifecycle of all incidents, ensuring an appropriate priority is applied to them, escalating as required to an appropriate line of support and communicating progress to the Authorised User. An ancillary feature of this structure is the collection and collation of incident trend data to support effective Problem Management. The SPOC will act as the communication hub between Authorised Users and technical support elements within the Contractor.

5 Technical Application and Infrastructure Support

The Contractor shall deliver application and infrastructure support by integrated teams, as detailed in Figure 2. Technical support shall be available to respond to service incidents, problems and requests on a 24/7 basis.

5.1.1 1st Line Support

The Service Desk assumes responsibility for all 1st Line technical support for reported Incidents by conducting the following activities:

- Incident logging and acknowledgment, ensuring all relevant information has been provided.
- Incident categorisation and prioritisation.
- Initial diagnosis; validation of an Incident to identify the scope of the requirement, to establish if it is related to user permissions, access control, change requirement or non-conformance and whether escalation to Second Line is required.
- Escalation, if necessary, to 2nd or 3rd Line support.
- Incident resolution: the Service Desk personnel are suitably qualified and experienced to conduct first line diagnostics on DES AIMS (e.g. using the SOLARWINDS tool for network performance).
- Incident closure; by applying a routine resolution (as applicable to Service Desk skillset and experience).
- Communication with the Authorised Users throughout the life of the Incident.

[Redacted]

Figure 2: Application and Infrastructure Support

5.1.2 2nd Line Support

Where an Incident or Request is beyond the capability of the Service Desk, as it involves a more complex resolution that requires an elevated level of skill, training and experience, it will be escalated to 2nd Line technical support. The Technical Team, comprising software analysts, developers, testers and release/deployment engineers, overseen by the Service Operations Technical Lead, will be engaged to confirm initial diagnosis and conduct incident resolution and closure. Further diagnosis at 2nd Line involves deeper analysis to validate the Incident to confirm the scope of the requirement and to establish if it is a change request or non-conformance. Investigative activities may include the replication of incidents or problems on a representative test system, capture steps to reproduce and establish if the Incident is across multiple Air Systems or related to a specific capability or role, or if related to a configuration, data or software code issue. Based on the outcome of investigation, a minor configuration change will be addressed by Second Line resources, whereas a major resolution will be escalated to Third Line.

5.1.3 3rd Line Support

3rd Line support will engage both the Technical Team and internal and external infrastructure support elements, as necessary. It will expand the 2nd Line investigation findings and determine the root causes, using product designs, code or specifications and, if applicable, may require the support of external organisations, such as the Contractor's sub-contracted hosting partner (Babcock Analytic Solutions (BAS)), who will be engaged through the Infrastructure and Security (I&S) Team. The outcome of such an investigation will confirm if a minor or major resolution is required and a subsequent and appropriate resolution will be provided in accordance with the Contractor's change management process.

An extension to the 3rd Line support available to the DES AIMS Service, will involve the Contractor collaborating with the Contractor's sub-contracted hosting partner BAS, utilising ITIL Incident, Problem and Event Management best practices, to enable successful escalation of infrastructure events between 2nd and 3rd Line support experts and between organisations. The I&S Team utilises a dedicated Help Desk tool internally within the business, to track and manage any infrastructure incidents. The proactive monitoring system enables automated alerting to help ensure that any incidents or events result in minimal impact to the Authority. Any impact to the DES AIMS service will be reported to the affected Authorised Users using the Online Support Facility. System performance & availability, including the supporting utilities (e.g. electrical supplies) are actively monitored by both the Contractor and its sub-contractor BAS: these systems monitor CPU and Memory Load as well as disk space utilisation. the Contractor and sub-contractor, BAS independently and actively monitor the system to ensure the desired uptime and service availability is maintained. Critical and warning events that are detected by monitoring systems are logged by the Service Desk and managed through the Incident or Problem Management processes.

6 Technical Support Processes

The Contractor notes that all levels of support apply ITIL best-practice, which are underpinned by a series of processes embedded and detailed in the Company's ISO9001 certified Quality Management System. The Contractor has invested in external ITIL training and mandated that members of the Contrator's support team are ITIL-trained and able to promote best-practice throughout the Contractor's Service Management Team.

6.1 Incident Management

The Contractor shall apply an Incident Management process providing resolution to unscheduled service interruptions, in order to maintain a high quality of service. Authorised Users report Incidents to the SPOC via telephone or through the Online Support Facility. An appropriate resolution route is taken, depending on the scope and scale of the incident.

6.1.1 Incident Categorisation and Prioritisation

The Contractor shall categorised and prioritise Incidents as Levels 1 to 4, depending on the number of Authorised Users affected and the assessed impact, as detailed in Table 1. This triaging system aims to minimise the time that an incident affects the Users' ability to utilise all functionality within DES AIMS. The performance metrics associated with Incident resolution are detailed in the DES AIMS Service SLA at Annex A.2 to Schedule 11.

[Redacted]

Table 1: Incident Categorisation and Prioritisation Matrix

6.1.2 Initial incident diagnosis

The Service Desk conducts 1st Line diagnosis by analysing the symptoms provided through the Online Support Facility or by communicating directly by telephone with the originator of the incident. An initial validation of an Incident is carried out to identify the scope of the requirement and establish if it is related to user permissions, access control, a change requirement or non-conformance, escalating to Second Line as required.

6.1.3 Incident escalation

The Service Desk will escalate an incident for 2nd or 3rd Line technical support if it requires a more complex resolution, necessitating an elevated level of skill, training and experience. Should a major disruption to service be reported, the Service Desk will contact the I&S Manager to initiate Business Continuity or Disaster Recovery actions.

6.1.4 Incident Investigation and full diagnosis

The Service Desk provides 1st Line investigation of routine Incidents. For the more complex incidents, the 2nd or 3rd Line support elements are utilised, as described in paragraph 5.

6.1.5 Incident resolution

The Service Desk will provide a resolution if it is within their capability; otherwise, the escalation to 2nd or 3rd Line support for investigation and full diagnosis will mobilise the more experienced and knowledgeable members of the Technical Team to develop a suitable resolution. When fully developed, a test and validation process is applied. A successful test and validation programme is followed by preparation of deployment packages, which are released to pre-production environments for final verification, prior to release to the production environment.

6.1.6 Incident closure

Successful resolution to the satisfaction of the originator will result in formal closure of an incident. Performance metrics will be captured to inform the Service Level Agreement reporting process. Trends or repeated incidents will be fed into the Problem Management process for root-cause analysis and long-term resolution.

6.1.7 Communication

The SPOC will maintain communication with the Authorised Users throughout the life of the Incident, by either telephone or by updating the status within in OSF.

6.2 Problem Management

Through the analysis of previous incidents and the associated technical resolution activities the Service Desk will identify and report any trends in incident causes to the Technical Team. These causes will be addressed under the Problem Management process. The individual elements of the Technical Team (e.g. analysts, developers and testers) and, if necessary, infrastructure specialists will be engaged, depending on the types of problem encountered, to analyse and diagnose a root cause and to identify and implement permanent solutions in the following ways:

- Categorisation & prioritisation – impact and trend analysis conducted to define if a major or minor problem exists:
- Minor problems are pre-approved, whereby they will be integrated into the programme plan without in-depth assessment.
- Major problems, requiring wider assessment and impact analysis, follow the full change management process.
- Investigation & diagnosis – identification of a root cause.
- Problem resolution – implementation of an appropriate solution in accordance with the Contractor's change management process.
- Problem review & closure – A review of the effect of a resolution to allow closure.

6.3 Change management

Requirements for changes to the DES AIMS service will be managed through a change management process, aligned with ITIL best-practice. The Contractor operational programme (TOP), shown in Figure 3, comprises a comprehensive set of change management processes.

[Redacted]

6.3.1 Capture & Assess

Captured through the Online Support Facility as a request for change , changes are initially assessed and then presented to the Contractor'schange assessment b (CAB).

6.3.2 Plan & Approve (Change Planning)

Contractor's CAB-approved changes are integrated into the Service Transition Operational Road Map (STORM) using the Contractor's dedicated planning tool, where appropriate resources are allocated.

6.3.3 Prepare, Realise & Integrate (Change Implementation)

Implementation involves analysis of the change, producing low-level requirements for development. When fully developed, a test and validation process is applied, after which full regression testing is conducted. Deployment packages are released to pre-production environments for final verification, prior to release to the production environment.

6.3.4 Change Implementation (Prepare, Realise & Integrate)

The implementation phase commences with an analysis of the change, which produces low-level requirements for development. When fully developed, a test and validation process is applied by the Contractor, after which full regression testing of the service is conducted. A successful test and validation programme is followed by preparation of deployment packages, which are released to pre-production environments for final verification, prior to release to the production environment. All changes are recorded and tracked in a configuration management database.

6.4 Service Requests

The DES AIMS Service provides a 24/7 Online Support Facility for Authorised Users to raise Service Requests which comprise either an Access Management or Request Fulfilment task. Access Requests grant Authorised Users the rights to utilise a service, whilst preventing unauthorised access. Tasks include managing access to services, permissions; groups and roles. Request Fulfilment is the process to handle requests for information, advice or access to a service. These tasks include password management, requests for an administration task (e.g. archiving, data export) or conducting a minor change to Sys Admin configuration (e.g. amend user look-up lists). A full description of the System Administration Support Service is detailed at Annex B to Schedule 11 of SC2.

Annex A.2 to Schedule 11 –Service Level Agreement

1 Introduction

This document details the Service Level Agreement (SLA) for the Contractor provided DES AIMS service; it explains the key services provided and the quality principles (contained in JSP604, DEF STAN 05-138, ISO27001/2) delivered to provide Authorised Users with the contractually agreed service levels. the Contractor' performance will be measured by the Authority on a monthly basis and used to justify service payments and any remedial action required.

This SLA sets out the following:

- The services provided to DES AIMS Authorised Users
- The overall standards to be achieved covering:
    - Service availability
    - System availability
    - Performance levels
    - Incident resolution times
    - Service Level reporting metrics
    - Service Credits
- How the SLA will be managed, measured and reported
- he mechanism for addressing any problems related to the provision of the DES AIMS service

The statement on User Access controls is provided as a separate document and provided at Schedule 15.

2 Objectives of the Service

The objective of the service provided by the Contractor is to meet the requirements detailed within schedule 2 Statement of Requirements - Part C DES AIMS Service Requirements, which are detailed under the following schedule headings:

- C.1 – Service
- C.2 – Technical Support
- C.3 – Service Levels
- C.4 – System Administration Support Services
- C.5 – Business Continuity and Disaster Recovery
- C.6 – Contract Management Reporting
- C.7 – Exit Strategy
- C.8 – New user and Top Up Training
- C.9 – Additional Services

3 Responsibilities

The Contractor shall provide the DES AIMS service under the direction of the Contractor's Service Management Team. An Account Manager is allocated by the Contractor to this service and is the point of contact for all enquiries from the Authority on Service performance or contractual matters. The Account Manager will attend the Monthly Contract Management meetings at the Authority's Offices in Bristol. The Authority will endevour to give 10 days notces before the monthly contract management meeting.

[Redacted]

If any issues cannot be resolved to the Authority's satisfaction by the DES AIMS Account Manager they will be escalated to the Service Management Team to agree a path to resolution with the Authority.

4 Service Level Agreement

The DES AIMS service shall have a Service Availability of 99.6% and a System Availability of 99.6%. The service provided by the Contractor shall meet the needs of the Authorised Users and be fully scalable to meet required changes in Authorised User numbers in increments of 50 users. The Service Desk is easily scalable to provide or withdraw additional Service Desk and Training capacity, as required, depending on the resource requirement.

The DES AIMS application sits behind a load balancer, which monitors the load on the web servers and allows for traffic to be directed to the server with the least load. It provides caching of popular content, such as images which do not change frequently, thus enabling faster response times and lower load on the back-end servers. This allows response times to be optimised even with additional Authorised Users, technically there is no limit on the number of Authorised Users. The hosting site also provides plug in server capacity that will allow additional storage capacity to be allocated to accommodate additional users creating additional records.

4.1 Service Availability

The DES AIMS service provided by the Contactor shall be available to the Authorised Users on a 24 hour basis for 365 days-a-year to the agreed availability level below. At contract award the service will support 6,300 Authorised Users located across 26 Air Systems and 17 locations. Service Availability in this context is defined as an Authorised User being able to access the DES AIMS service at the performance levels that meet the ability to:

- Login to the system within 5 seconds
- Loading the front page within 5 seconds
- Loading of a blank issue /entity form / screen within 5 seconds
- Loading of main user dashboard within 10 seconds
- Returning search results of a query within 10 seconds

4.1.1 DES AIMS User Access Service Availability

The minimum performance required in accordance with Annex A to this SLA will be maintained. The Agreed Service Time (AST) will be calculated on a monthly basis according to the following formula:

Agreed Service Time = (24 hours x Calendar Days in the Month) – (Hours PDT) – (Hours DTOS)

Planned Downtime (PDT) is defined as those periods of planned maintenance where the Authority has been given at least 3 days' notice. Any system will require pre-planned maintenance, and this will be kept to the minimum required and conducted where possible out of normal working hours.

Downtime Other Systems (DTOS) is defined as downtime whether planned or unplanned for those systems outside the control of the Contractor i.e. MoDNET. the Contractor monitors notifications from the Global Operations and Security Control Centre (GOSCC) Planned Outage Cell and will notify Authorised Users when any outage will affect the DES AIMS service.

Service Availability is calculated based on the Agreed Service Time (AST), and the unplanned downtime (UDT), according to the formula.

$$\text{Service Availability} = \frac{AST - UDT}{AST} \times 100\%$$

Unplanned Downtime (UDT) is defined as any period of time where an Authorised User is unable to access the service outside those identified in PDT and DTOS.

Availability will be actively monitored by both the Contractor and its sub-contractor Babcock Analytic Solutions (BAS); these systems monitor CPU and Memory Load as well as disk space utilisation.

4.1.2 Training Service Availability

The training available for DES AIMS as provided by the Contractor is detailed in the Training Plan and explains the methods used predominantly Instructor-Led, On-Line and Integrated User Guides. The Online and Integrated User Guides are available continuously. The Instructor-Led training will be advertised through the online support facility for Authorised Users to book places.

The service has been contracted by the Authority to provide capacity to train 1500 new users per year. The throughput is expected to fluctuate month on month and the service must be prepared to surge as new groups of users require training. Therefore, to limit the exposure to fluctuation provision has been made to be able to deliver up to 180 Instructor-Led training places in any one month.

Information will be provided monthly on the number of new users that have received training against the number of new users created. Top-up training in the main will be achieved using the online method; information on the levels of users accessing this will also be made available to the Authority after each major change to DES AIMS.

4.2 System Availability

System Availability is defined in the ITT as the full functionality of the toolset being available to all Authorised Users. The Contractor endeavours to maximise the time that this is achieved by applying quality processes to any required releases and actively monitor for any impact on the quality of service.

The Contractor's Service Desk prioritises incidents and where appropriate applies workarounds to restore the service functionality until such time as a final resolution is delivered. This workaround allows Authorised Users to conduct their full range of functions albeit potentially using slightly different methods to the normal operating process.

System Availability is calculated according to the following formula:

$$System\ Availability = \frac{AST - ITL}{AST} \quad x100\%$$

Agreed Service Time (AST) is the same calculation as for Service Availability in paragraph 4.1.1 above.

Incident Time Lost (ITL) is the hours lost due to an incident prioritised in any of the P1-P4 categories as identified in paragraph 4.4 that have exceeded the given resolution time.

4.3 Performance Levels

The required performance levels for Authorised Users utilising the DES AIMS service have been defined and are listed below:

- Performance levels that meet the ability to:
    - Login to the system within 5 seconds
    - Loading the front page within 5 seconds
    - Loading of a blank issue /entity form / screen within 5 seconds
    - Loading of main user dashboard within 10 seconds
    - Returning search results of a query within 10 seconds

Through the use of two different Proactive Monitoring Systems, Solarwinds and Ipswitch WhatsUpGold which are located at two differently ALI connected sites, the Contractor is able to monitor the performance of the AIM Service continuously. This is completed by using a combination of SNMP (Simple Network Management Protocol) and WMI (Windows Management Instrumentation). The monitoring system uses a number of different monitoring techniques, these include:

- "Active" Monitors, where by the system queries a network service and waits for a response, if the response is as expected then the service is deemed up, through careful tuning, the monitoring systems are able to detect variations in the responses and as such alert the support organisations.
- "Passive" Monitors, unlike Active monitors, passively listen for events on a device, when a particular "event" occurs, comprehensive debug information is available which is especially useful as events can occur at any time.
- "Performance" Monitors, are used to gather important information about the utilisation and availability of the different aspects of the services, a combination of CPU/Memory/Interface/Ping and Disk Utilisation is used. This helps to ensure that the service is appropriately scaled to the Authority's requirements.

This solution provides a holistic view of the all parts of the Instructure which is under the configuration control of the Contractor and its supply chain. The Contractor's monitoring service operates on a continuous basis and has the ability to alert support staff at each Organisation (the sub-contractor BAS & the Contractor) enabling problem resolution in a timely manner.

By using a combination of all three monitoring mechanisms, a deep understanding of MOD networks, and having designed the platform from the ground up, it can be determined whether an incident is related to the hosting platform, application or is outside the control of the Contractor. In the event the incident is outside the control of the Contractor an incident will be raised with the Authority PoC.

4.4 Incident Resolution Times

Incidents will be reported to the Contractor using the On-line System and will be processed in line with the process detailed in Annex A.1 to Schedule 11 Technical Support. The severity of the incidents are described in Table 1 below and the aim is to use this triaging system to minimise the time that an incident is affects the Authorised Users' ability to utilise all functionality within DES AIMS.

[Redacted]

Incidents reported through the online support facility will be accepted by the Service Desk and receipt will be acknowledged within one hour. For all incidents a management owner will be assigned in line with the agreed procedure.

As the incident progresses the incident record on the Online Support facility will be updated to show progress and also an expected time for resolution. This is important to ensure the Authorised User can plan their work and also provide any additional information to the Service Desk. Where the incident affects multiple users, the Contractor will post alerts on the Online Support Facility.

4.5 Problem Management

An integral part of incident resolution is to identify any trends and analyse the root causes thus highlighting any underlying problems that need to be investigated and resolved. Once resolved the problem should not re-emerge and a performance measure to monitor this is included.

4.6 Security

Both the Contractor and its sub-contractor BAS utilise the Defence Out-of-Band Update Service (DOBUS) to ensure security updates, including anti-virus definitions, are applied across the infrastructure. These patches will be installed as they become available from the appropriate sources. Where the DES AIM Service uses Open-Source components, the Contractor will actively monitor Common Vulnerabilities and Exposures (CVE) databases for new security vulnerabilities and take required action to mitigate the risk to the Authority's data. When security patches are received, they shall be applied to the DES AIMS infrastructure.

In the event of a Security incident, which could affect the operational effectiveness of the DES AIMS System or result in data loss or leakage, the Contractor will report the incident to

the Authority via email to the nominated DE&S PoCs or mailbox(es) within twenty minutes of the incident being detected. The Contractor will also report the incident through MOD Security Incident Reporting System (MSIRS), which is a requirement of ALI Code of Connections (CoCo), while also liaising with MOD Computer Emergency Response Team (MODCERT), Joint Security Co-ordination Centre (JSyCC), Industry Warning and Reporting Point and DAIS, in line with conditions laid down in JSP440. Any security incident which may affect either the Contractor systems or DES AIMS will be recorded and managed through the the Contractor ISO27001 authorised Incident and Breach Reporting Policy.

4.7 Service Level Reporting Metrics

See Appendix A to Annex A.2 to Schedule 11 which lists eight service level performance measures.

4.8 Service Scaling

The DES AIMS service offered is scalable, up or down, in increments of 50 Authorised Users whilst maintaining the service availability at the agreed performance levels in the SLA.

4.9 Service Credits

The DES AIMS service performance will be measured every month using the 14 measures in Annex A. If more than one performance measure is not achieved in any one month the Service Credit of 5% of the Monthly Service Fee will be applied to the following month's service charge.

Where the same performance measure fails to be met for three months in a row the Service Credit of 5% of the Monthly Service Fee will be applied even if that is the only measure that is not achieved.

The Contractor is responsible for measuring the performance against the SLA and presenting these to the Authority to be considered at the monthly Contract Management meeting.

Occasionally, the cause of service level failures will be outside the control of the Contractor; consequently, the following conditions apply:

- Specific acts or omissions by the Authority or its Authorised Users that cause a service level failure are excluded from the service level performance calculations
- Where the failure relates to aspects outside the control of the Contractor such as the availability of non the Contractor infrastructure (i.e. MODNET/DII) then these will be excluded from the service level performance calculations
- When the sample size that is used for calculating for the service performance is small, any deviation can have a significant impact on performance. For example, two events with one pass and one a fail will lead to performance of 50%. Therefore, where the number of events is fewer than 20, the performance for service credit purposes will be assumed to be 100%. The performance in this instance can be reviewed over a longer three month period of time to ensure the Contractor is not penalised for a small sample size and to judge the longer term performance trend.

Appendix A to Annex A.2 to Schedule 11 – Service Level Agreement - Metrics

[Redacted]

Annex B to Schedule 11 – System Administration Service Level Agreement

1 Introduction

This document details the Service Level Agreement (SLA) for the the Contractor provided DES AIMS System Administration support service in accordance with Schedule 2, Part C – The DES AIMS Service Requirement, at C.4 – System Administration Support. The Contractor' performance will be measured by the Authority on a monthly basis and used to justify service payments and any remedial action required.

The SLA provides a comprehensive overview of the routine System Administration services provided and explains how the Contractor will support the DES AIMS Service and its 6,300 Authorised Users, across 26 Air Systems and 17 MoD sites, specifically:

- The range and type of services
- Details of the the Contractor System Administration team
- Performance levels
- Service Request resolution times
- Service level reporting metrics
- Service capacity levels

Verification of each service request shall be provided by the Authority, to ensure Authorised Users are permitted to hold the levels of access requested and have legitimate business reasons to do so.

2 Service Concept

The DES AIMS System Administrative support service combines two areas of ITIL best-practice within a single service, available to Authorised Users through submission of a Service Request to the DES AIMS Service Desk. The Service Desk operates as the Single Point of Contact (SPOC) for the Service:

- Access Management - The process which grants Authorised Users the rights to use a service, whilst preventing unauthorised access; access management tasks include:
    - Adding, amending or removing access and entry to services, data and facilities.
    - Assigning or amending rights or permissions that Authorised Users can exercise, such as read, write, execute, change or delete.
    - Managing groups and roles that Authorised Users are assigned to.

- Request Fulfilment - The process to handle Service Requests from Authorised Users to request information, advice or access to a service; request fulfilment tasks include:
    - Account password management.
    - Requests for an administration task to be undertaken, e.g. archiving or data export.
    - Conducting minor changes to System Administration configuration, e.g. amending user look-up lists.

3 System Administration Support Services

3.1 Range and Type of Services

A comprehensive range of services is provided that enables the 6300 Authorised Users to seek System Administration support to satisfy the primary Authority requirements detailed in Schedule 2, Part A – DES AIMS software requirement, at A.5 – System administration functionality to maintain DES AIMS.

Due to the potentially sensitive nature of the System Administration services, Access Management best-practice recommends such activities require verification that an individual who requests access to services is permitted to hold such levels of access and has a legitimate business reason to do so. All Service Requests will need to be verified by a designated Authority representative prior to submission and any that have not will be returned. The Service Desk will satisfy a requirement within the appropriate Service Request response times detailed in this SLA (Annex B to Schedule 11).

3.1.1 Add, Change or Remove Authorised Users

The policy for the control of access for Authorised Users is defined in Schedule 2, Part C – DES AIMS Services, at C.3 User Access Control, but, specifically, System Administration support shall provide the following Authorised User access control service:

- Add or Change Authorised Users - The the Contractor SPOC will create new Authorised User accounts or an amendment to an existing account, following receipt of a Service Request accompanied by an Authority-approved User Account Application. The Authorised User will be provided with a DES AIMS role account, within one of the four User Types defined in C.3 User Access Control, a user name and temporary password by e-mail from the Service Desk along with instructions in the use of DES AIMS. The bulk creation of new Authorised User accounts during the introduction of a whole new Air System or Delivery Team will be excluded from Service Request SLA performance reporting metrics.
- Remove Authorised Users - A monthly Service Request will be raised by the Authority providing a list of all DES AIMS accounts to be removed. A specific Service Request will be made if the immediate removal of an account is needed for the purposes of data protection.

3.1.2 User Account Password and Profile Management

System Administration support will be provided for Authorised User password or profile management, through:

- Service Desk - Service Requests will be submitted to the Service Desk for account password resets and Authorised User profile updates, including changes to title, rank, e-mail, contact number or department. The Authorised User will be provided with a temporary password or details of the profile updates requested by e-mail from the Service Desk.
- Self-Service - password changes and profile updates can be carried out by the user through the ‘Profile’ section within the DES AIMS application.

3.1.3 Define and Set Permission-level Groups for Authorised Users

A Service Request may be made for the creation of specific permission-level Groups within DES AIMS; designated roles can be included in these groups and individuals assigned accordingly. The parameters for such Groups shall be approved by a designated Authority

representative prior to the Service desk applying the necessary actions. Large-scale changes to Groups, resulting from Authority organisational changes will be excluded from performance reporting metrics, unless they are as a result of changes to MAA Regulations or Air Environment Policy.

3.1.4 Conduct Archiving Activities

To progress an entity within DES AIMS from 'Closed' to 'Archived', where an Authorised User with the appropriate permissions is not available, a Service Request can be submitted for the activity.

3.1.5 Set-up and Maintenance of User Look-up Lists

The Service Desk is able to satisfy requests for the set-up and maintenance of User look-up lists within DES AIMS. Creating a new look-up list or adding new items to an existing look-up list is carried out without any risk to data integrity. Confirmation of completion of the activity is provided to the Authorised User.

The removal of existing items in a look-up list could affect the integrity of associated data and requires resolution by 2nd or 3rd Line Support. Service Requests for amendments to look-up lists that have a significant impact on data integrity are excluded from the SLA performance reporting metrics and are resolved as Non-routine Service Requests. These will be satisfied within a reasonable timescale, to be agreed with the originator based on the complexity and urgency of the task.

3.1.6 Export of Bulk data from DES AIMS

Service Requests for the export of bulk data from DES AIMS will be satisfied by the Service Desk on a case-by-case basis, timescales will depend on the scale and complexity of the export request but will be no longer than 10 working days.

Any request for the bulk export of the complete DES AIMS database shall be requested separately by the Authority under the DES AIMS Data Migration Vision for the Future document provided in the ITT in the Dataroom that states at any point throughout the contract period, the Contractor shall provide all DE&S data and attachments in an SQL Server format database within 10 working days of a request.

3.1.7 Define, Approve & Set Each Authorised User's Permission, Authority & Access Rights

Closely aligned with the creation of new User accounts and the amendment of existing accounts, the definition and approval of an Authorised User's roles, permissions and access rights are submitted on a DES AIMS User Account Application and approved by a designated Authority representative before submitting a Service Request to the DES AIMS SPOC for action.

3.1.8 Non-routine Service Requests

The DES AIMS System Administration Support Service is responsible for satisfying routine system administration tasks in accordance with the primary Authority requirements in Schedule 2, Part A – DES AIMS software requirement, at A.5 – System Administration functionality to maintain DES AIMS. Service Requests received by the SPOC that are non-routine will be satisfied within a reasonable timescale, to be agreed with the originator based on urgency and impact, but will be discounted from any performance reporting metrics due to

the scale or complexity of the task. An example of a non-routine Service Request is a large-scale change to User Groups following an internal re-organisation within a Delivery Team, which has not been prompted by a change in MAA Regulations or Air Environment Policy.

3.1.9 Out-of-Scope Requests

Should a Service Request be deemed to be a task outside the scope of the DES AIMS System Administration Support Service requirements the originator will be contacted to revise or withdraw the requirement. Examples of out-of-scope requests include the following:

- Reporting an Incident (e.g. Authorised User account corrupted).
- Request for training of any kind.
- Request for Additional Services.

The Authorised User will subsequently be directed to raise the appropriate request through the correct channels. The original Service Request will be closed at that point and will be excluded from any performance reporting metrics.

3.2 Service Support Team

The DES AIMS Service Desk acts as the SPOC for System Administration Service Requests and the provision of unified communications to the user base. All UK-based support staff are experienced in their field, SC-cleared and have detailed knowledge across Service modules. They are trained internally and assessed as competent in the use of the System Administration Toolkit before being allocated System Administration rights and deployed on satisfying the range of System Administration requests associated with the DES AIMS Service.

Should a Service Request be deemed to be an exceptional request (i.e. may affect data integrity), the Service Desk has the ability to escalate it to 2nd or 3rd Line support. A collaborative working relationship exists between technical and customer support experts within the dedicated Service Operations Team. The Service Desk is resourced to ensure a full System Administration Support Service is provided to the 6300 DES AIMS Authorised Users, with the flexibility to scale the resource as required to react to increases or decreases in the Authorised User base or handover of System Administration responsibility to DE&S.

3.3 System Administration Tools

3.3.1 System Administration Toolkit

A comprehensive System Administration Toolkit will be provided, which provides the Service Desk with the necessary permissions and administration functionality to satisfy the DES AIMS System Administration Support Service requirements. Initially, access to the Toolkit is limited to the Contractor Service Desk operators who are fully-trained and competent in the use of the Toolkit. However, if the Authority takes the option during the contract term to assume responsibility for DES AIMS System Administration Service designated Authority representatives will be trained and competent to use the System Administration toolkit. On completion of the handover and on an agreed date, the Contractor System Administration will cease responsibility for System Administration support and will only access the System Administration Toolkit for maintenance and incident resolution purposes.

3.3.2 Self-Service Capability

Exceeding the primary Authority requirements for the System Administration Support service, the the Contractor solution provides a self-service capability within the DES AIMS Online

Portal, whereby an Authorised User can undertake a range of Authorised User account administration tasks, such as password changes and user profile updates (title, rank, e-mail, contact number, department). This functionality reduces the administration burden on the System Administration Support Team, with the long-term view focussed on the Authority assuming responsibility for System Administration support at a point in the future, necessitating a reduced Authority resource to operate the service.

4 Performance (C.4.2)

4.1 Service Availability

All System Administration support will be requested through the SPOC, where the Service Desk shall handle all System Administration Service Requests. System Administration support will be available to Authorised Users through provision of the following:

- A dedicated Service Desk contact telephone number (details to be advised during Service Implementation) operational with effect from 01 April 2019 and available Monday to Friday (excluding public holidays) between the hours of 7:00 am and 7:00 pm. The call will be logged by the Service Desk as a Service Request.

- An Online Support Facility, operational with effect from 01 April 2019 and accessible from MODNET and approved Industry partner IT systems, through which System Administration Service Requests can be submitted. The online facility shall be available 24 hours a day, 7 days a week. However, any Service Request submitted through the Online Support Facility outside of the normal Service Desk telephone operating hours (Monday to Friday (excluding public holidays) between the hours of 7:00 am and 7:00 pm) will be processed the next working day.

- A self-service capability within the DES AIMS application itself, operational with effect from 01 April 2019 and available 24 hours a day, 7 days a week, where an Authorised User may themselves conduct a range of Authorised User account administration tasks, such as password changes and user profile updates (title, rank, e-mail, contact number, department).

4.2 Service Request Resolution Times

Service Request resolution times are measured from the point that an acceptable Service Request, complete with relevant supporting documents and/or information, is received by the Service Desk to the point of satisfaction of the request where the originator has been informed. Measurement shall not commence if a Service Request is incomplete or out of scope of the System Administration service.

Any measurement period is subject to the bounds of the Service Desk operating hours of Monday to Friday (excluding public holidays) between the hours of 7:00 am and 7:00 pm. As an example, should a Service Request with a SLA response time of twenty four (24) hours be received by the Service Desk on a Friday at 6:00 pm and satisfied by 10:00 am on a Monday morning, the response time shall be measured as four (4) hours for performance reporting purposes. The DES AIMS System Administration Support Service Request resolution times are detailed in Table 1.

4.3 Performance Reporting

The Contractor is responsible for collating data to measure performance and will report

performance against the SLA targets monthly to the Authority, highlighting where and why any Service Requests have been excluded from the performance metrics.

The metrics to be applied to this SLA for each reporting month are:

- 95% of Service Requests shall be satisfied within the resolution times detailed in Table 1.

[Redacted]

4.4 Service Credits

Where the DES AIMS System Administration service fails to meet the required level for three consecutive months the Service Credit of 5% will be applied to the following month's System Administration service charge.

Occasionally, the cause of service level failures will be outside the control of the Contractor; consequently, the following conditions apply:

- Specific acts or omissions by the Customer or its Authorised Users that cause a service level failure are excluded from the service level performance metrics.

- Where the failure relates to aspects outside the control of the Contractor such as the availability of non-Contractor infrastructure i.e. MODNET/DII, then these will be excluded from the service level performance metrics.

- When the sample size that is used for calculating the service performance is small, any deviation can have a significant impact on performance i.e. two events with one pass and one a fail will lead to performance level of 50%. Therefore, the Contractor propose that where the number of events is 19 or fewer the performance for service credit purposes will be assumed to be 100%. The performance in this instance can be reviewed over a longer three month period of time to ensure the Contractor is not penalised for a small sample size and to judge the longer term performance trend.

5 System Administration Support Service Handover Plan

If the Authority wishes to invoke the handover of the System Administration Support Service the Contractor will transition the service in line with the process detailed in the Handover Plan which is a separate document.

6 Service Capacity

The System Administration Support Service is already established to provide support to 6,300 Authorised Users, through the application of an appropriate level of trained and experienced the Contractor staff and robust tools, based on 10 years' experience of supporting the existing AIMS service. As the current service has expanded, the Service Desk capacity has been enhanced to accommodate an increasing numbers of Authorised Users. This has been achieved through development of internal training packages and standard operating procedures for the System Administration function, managed within the Contractor's Quality Management System.

A suitable level of additional support resources will be available to augment the DES AIMS

System Administration Service in the event of an incremental increase in the number of Authorised Users above 6,300, in increments of 50 Authorised Users. The same training, processes and procedures will be applied to the Service to ensure the requisite range of System Administration tasks can be satisfied within the timescales detailed in this SLA. Conversely, the service may be scaled back accordingly, in the event the number of Authorised Users decreases, in decrements of 50 Authorised Users.

Similarly, capacity may be adjusted to cater for a change in the scope of System Administration tasks and responsibilities, over and above those detailed herein. The System Administration Toolkit will have the capacity to manage any increase in the number of Authorised Users. The overall System Administration Support Service is scalable to balance team-size versus response times, with flexibility to adapt to a change in scale either way.

7 Handover plan

The handover plan as per the Contractors' Invitation to Tender proposal shall apply if the Authority requests a handover of the System Administration Support Service to the Authority.

Schedule 12 – Business Continuity and Disaster Recovery

1. The Business Continuity and Disaster Recovery (BCDR) Schedule ensures the continuity or the recovery of the business processes and operations following any failure or disruption of any element of the DES AIMS service in accordance with Schedule 2.

2. The BCDR Plan is provided at Annex A to Schedule 12 and provides the plan in reaction to failure or disruption or disaster recovery. A disaster here shall mean the occurrence of one or more events which, either separately or cumulatively, mean that the DES AIMS service will be unavailable for a period of twenty four (24) hours or which is reasonably anticipated will mean that the provision of the DES AIMS service or a material part thereof will be unavailable for that period. The BDCR Plan shall detail the processes and arrangements that the Contractor shall follow to:

    a. ensure continuity of the business processes and operations supported by the DES AIMS service following any failure or disruption of any element of the DES AIMS service; and

    b. the recovery of the DES AIMS services in the event of a Disaster.

3. The BCDR Plan shall:

    a. set out the general principles applicable to the BCDR Plan;

    b. relate to business continuity; and

    c. relate to disaster recovery.

4. Review and Amendment of the BCDR Plan

4.1 The Contractor shall review the BCDR Plan:

    a. on a regular basis and as a minimum once every six (6) months; or

    b. as requested by the Authority.

    c. each review of the BCDR Plan shall be a review of the principles and processes set out in the BCDR Plan. It shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Contractor within the period required by the BCDR Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Contractor shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Authority a report (a Review Report) setting out:

        i. the findings of the review;

        ii. any changes in the risks associated with the provision of Contractor Deliverables; and

        iii. the Contractor's proposals for addressing any changes in the risk and its proposals for amendments to the BCDR Plan following the review detailing the impact that the implementation of such proposals may have on DES AIMS service or systems provided by a third party.

Annex A to Schedule 12 – Business Continuity and Recovery Plan

1 Introduction

The purpose of this Business Continuity and Disaster Recovery (BCDR) Plan is to detail the activities that the Contractor conduct to ensure the continuity or recovery of the DES AIMS service following any failure or disruption of business processes or operations.

For the purposes of this plan a disaster shall mean the occurrence of one or more events which, either separately or cumulatively, result in the DES AIMS service being unavailable for a period of 24 hours.

When dealing with an Incident, any actions taken will be proportional to the type, scale and severity of the incident. Whilst the type, scale and severity of any incident is hard to predict, due to the nature of such events, the BCDR Plan outlines two of the most likely serious disaster scenarios, which would require the DES AIMS Service to enter a full Disaster Recovery (DR) cycle. The specific necessary technical recovery actions will depend on the initiating event; however, the principles laid out in this BCDR Plan remain the same.

The plan is based on a Recovery Point Objective (RPO) of 6 hours (100% of service capability and data recovered) and Recovery Time Objective (RTO) of twelve 12 hours or three and a half working hours (whichever is lesser) to restore to the agreed RPO or better.

To assist the Authority with confirming that the Contractor has met each of their requirements, this document includes reference in each paragraph header to the Authority's requirement serial numbers (e.g. C.5.1, C.5.2 etc) taken from Part C – DES AIMS Service, as per Schedule 2 of SC2.

2 BCDR Risk Register

A BCDR Risk Register is maintained and reviewed monthly by the Contractor and the Contractor's sub-contracted hosting provider Babcock Analytic Solutions (BAS), and provides a record of the perceived Risks to BC and the management, monitoring and maintenance of the Contractor's BCDR capabilities, including suggested improvements to preventative mitigations and recovery actions. It represents an assessment of the different kinds of risks and threats to the normal operating mode of the business and tracks the measures put in place to specifically mitigate those risks from occurring, specifically:

- Identify and assess all serious risks to the business
- Assess those risks to determine those that are above the acceptable threat level
- Document preventative measures already taken to mitigate against the perceived risks
- Identify further mitigating measures to prevent the risks identified from happening
- Plan and implement improvements to the preventative measures

3 Infrastructure Resilience

DES AIMS is hosted within the Keynsham Data Centre (KDC), in partnership with BAS. the Contractor has aligned this BCDR Plan with those arrangements that are currently in place with BAS and, where possible, the Contractor has introduced heightened levels of reliance to provide confidence in the service levels offered to the Authority.

The KDC site has a high-availability connection to the Assured LAN Interconnect (ALI), allowing for a complete failure of the Fujitsu-supplied router. A load balancer monitors the

load on the web servers and allows for traffic to be directed to the server with the least load. It provides caching of popular content, thus enabling faster response times and lower load on the back-end servers.

An accredited OFFICIAL-SENSITIVE (OS) network connected to the ALI is maintained at the the Contractor offices. DES AIMS data is replicated to a segregated area of this network to offer a fully functional alternative site, in the event that the KDC site does not survive a catastrophic incident. It also provides a near real-time replication of data, so that any service interruption is minimised in the event of a disaster. This capability is designed following the patterns set out in JSP604, with the ability to scale with minimal intervention and without incurring any service outage.

The accreditation status is maintained, through collaboration with Defence Assurance and Information Security (DAIS), Information Systems and Services (ISS) and Joint Cyber Unit (JCU), providing assurance that the network meets all the requirements of JSP604, and enabling the replication of DES AIMS data to the the Contractor OS network. The hosting environment is configured to allow for data replication.

A minimum of N+1 redundancy is provided within the infrastructure. Figure 1 contains a high-level network diagram covering both the KDC and the Contractor sites and the interconnectivity to enable successful business continuity to satisfy the RPO within the stated RTO.

The following services across the hosting environment comprise of at least N+1 redundancy:

- HVAC (Heating, ventilation, and air conditioning)
- UPS (Uninterruptible Power Supplies)
- ALI Connection
- Compute resource
- Redundant Disks
- On-Site Generators
- Web Servers
- Database Servers

[Redacted]

Figure 1: High-level Network Diagram

The DES AIMS Service can sustain multiple simultaneous component failures at both the physical and virtual level The design solution is based on proven virtualisation technologies and has the ability to load balance the web and database servers across different physical hosts,

4 Secure Data Backup

The Contractor's sub-contractor, BAS. provides 4-hourly database backups and daily full backups of the DES AIMS Service application data and Virtual Servers to tape, in order to facilitate data recovery. These tapes are stored both on and off-site in secure fire safes. All locations where DES AIMS data resides are Government secure facilities and have the ability to store and process classified Government information.

A proactive monitoring service is configured to alert the Support Organisations, at both the sub-contractors, BAS, and the Contractor's should any backup be missed or fail, after which

the Contractor will follow their ITIL-aligned Event Management procedure to ensure a timely response and appropriate corrective action is applied to reduce the likelihood of future occurrences.

5 Security Patching

Both the Contractor and its sub-contractor, BAS, utilise the Defence Out-of-Band Update Service (DOBUS) to ensure security updates, including anti-virus definitions, are applied across the infrastructure. These patches are installed as they become available from the appropriate sources. Where the DES AIM Service uses Open-Source components, the Contractor actively monitors Common Vulnerabilities and Exposures (CVE) databases for new security vulnerabilities and take action to mitigate the risk to the Authority's data. When security patches are received, they are applied to the DES AIMS infrastructure, as follows:

- Critical security patches within two weeks.
- Non-critical security patches, at a minimum of every six months.
- Major functional upgrades will be provided, at a minimum, once per year in agreement with the Authority.
- Incremental upgrades, as needed for fault resolution of incidents of Priority 3 and above.

6 Security Incidents

In the event of a Security incident, which could affect the operational effectiveness of the DES AIMS System or result in data loss or leakage, the Contractor will:

- Report the incident to the Authority via email to the nominated DE&S PoCs or mailbox(es) within 20 minutes of the incident being detected.

- Report the incident through MOD Security Incident Reporting System (MSIRS), which is a requirement of ALI Code of Connections (CoCo), and

    - Liaise with MoD Computer Emergency Response Team (MODCERT) and
    - Joint Security Co-ordination Centre (JSyCC) and
    - Industry Warning and Reporting Point and DAIS in line with conditions laid down in JSP440.

Any security incident which may affect either the Contractor systems or DES AIMS will be recorded and managed utilising the the Contractor ISO27001 Incident and Breach Reporting Policy.

7 Disaster Recovery

A disaster is defined as the occurrence of one or more events which, either separately or cumulatively, result in the DES AIMS service being unavailable for a period of twenty four (24) hours.

7.1 Incident Notification

An incident can be reported by DES AIM users, the sub-contractor BAS, MOD and the Contractor. Once the report is received the the Contractor Major Incident Manager (MIM) will carry out an initial assessment in conjunction with BAS as appropriate.

7.2 Initial Assessment

Before the DES AIMS Service enters the BCDR cycle, it is important to assess the nature and the extent of the incident. The the Contractor' Infrastructure and Security Manager, in conjunction with BAS, will ascertain the following before any action is undertaken:

- Has there been a complete loss of services?
- Is the nature of the disaster such that a relocation of the offices and services is required?
- Is there a requirement for a limited relocation of the affected systems and user base?
- Has there been a loss of server room(s) and what locations are affected?
- Has there been a loss of location(s) within the building and what locations are affected?
- Has there been a loss of IT services and what services are affected?
- Does the disaster impair the ability of site-based projects to conduct their business (albeit in a limited way)?
- Has there been a loss of key personnel?

These questions will be considered by both the Contractor and BAS to evaluate the situation and perform an initial assessment; the outcome of this assessment will be communicated to the Authority immediately.

7.3 Key Roles and Responsibilities

The Authority will decide whether to invoke the Disaster Recovery capability. Following receipt of a request to the Service Desk to invoke the Disaster Recovery capability from one of the Authority's nominated points of contact the Contractor' Local Response Team (LRT) will assemble, made up of available personnel comprising the following roles:

Major Incident Manager

The Major Incident Manager (MIM) will lead and manage the resolution of a major incident, and will undertake the following specific tasks:

- Carry out an Initial incident assessment
- Liaise with BAS
- Assign technical resources to the problem as required.
- Appoint personnel to the necessary roles, including a Deputy MIM, Communications Co-ordinator and Technical Lead.
- Act as a Point of Contact for senior the Contractor' staff.
- Inform senior stakeholders of the incident.
- Ensuring awareness amongst IT staff of their role and responsibilities.
- Maintain Incident Management Process documentation.

Communications Co-ordinator

The Communications Co-ordinator will maintain communications with the incident community, undertaking the following activities:

- Liaising with the Major Incident Manager for incident status updates.
- On-going liaison with BAS and MOD
- Establishing communications routes for all key stakeholders, both internal and external.

- Disseminating Initial, Update and Final Notifications to relevant parties.
- Maintaining an up-to-date list of contact details.

Technical Lead

The Technical Lead will co-ordinate the technical response to an incident, including the following:

- Liaison with the Major Incident Manager in developing a proposed resolution plan.
- Carrying out assessments of the technical requirements needed for systems recovery.
- Mobilising additional technical resources, as required.
- Managing the technical recovery of an incident.

Additional Personnel

Dependant on the scale, severity and complexity of an incident, additional personnel may need to be mobilised as required, including the following:

- Release Manager
- Programme Manager
- Development Manager

Contact details for key personnel are contained in the Contractor' contact register as a supporting document to this plan.

7.4 IT Operational Capability Assessment

The MIM will complete an Immediate Damage Assessment including an assessment of the status of key operational assets.

The MIM will assess the status of the services to the KDC server rooms as well as the actual servers and associated hardware located within the server room. The wider technical situation will be assessed to determine whether a full or partial recovery is required. Should an incident occur that results in the loss of any or all of the server rooms, affected stakeholders will be informed immediately.

A disaster scenario is categorised as one of the following:

- Scenario 1 - The KDC hosting site survives and is usable, either wholly or in part, with some IT infrastructure remaining.

- Scenario 2 - The KDC hosting site does not survive and none of the IT infrastructure remains.

Scenario 1 – Hosting Site Survives and is part or wholly useable

Short-Term Solution

Following the immediate damage assessment, a short-term solution is required for IT services to regain operational status. A flow chart showing the BAS short-term solution for restoring services is detailed in Figure 2

Figure 2: Scenario 1 – Short-Term Solution **[Redacted]**

Recovery of Server Services (if not already restored)

Both KDC the Contractor have access to the ALI, which provides flexibility and resilience for using either location to host OS applications and services.

Recovery of Data

Data will be recovered from backup tapes which are stored at various sites. Depending upon the nature of the incident it may be necessary to either:

- Transport backup tapes from Devonport.
- Use backup tapes held at Keynsham.
- Use a mixture of tapes held in Devonport and in Keynsham.
- Use an online connection to download data from Devonport.
- Transport backups from the the Contractor Offices.

Scenario 2 – Major - Hosting Site Does Not Survive

If, following an incident, the KDC has suffered a total loss of all facilities, the MIM will initiate and monitor action in accordance with BAS flow chart detailed in Figure 3. This procedure may be used to assist with the implementation of both a short-term and long-term solution.

Figure 3: Scenario 2 – Combined Short and Long-Term Solution **[Redacted]**

Short-Term Solution

A short-term Solution will be provided by the sub-contractor, BAS, using the Sungard AS Disaster Recovery Service. Sungard AS are contracted by the sub-contractor BAS to guarantee a five (5) hour response to supply appropriate equipment to enable reinstatement of the servers' function. Mobile recovery trucks loaded with appropriate equipment are located at a specified Business Recovery point near to appropriate Critical Power. A list of hardware requirements covers all KDC site server and communications equipment, the list is regularly updated when new equipment is installed. Fibre links for the ALI will be connected to the Sungard mobile recovery truck(s) to allow service provision to be resumed.

Supply of services by Sungard is recognised as a risk to business recovery, which is managed within the formal risk management system.

Long-Term Solution

Once major incident short term recovery has been implemented long term requirements will be reviewed in consultation with the Contractor's sub-contractor BAS to decide on the way forward.

Following a Major incident and once initial recovery has been completed a detailed review will take place, in consultation with all parties, to agree the revised Business as Usual requirements.

7.5 Recovery Process and Timeline

The timeline for recovery to meet the Recovery Point Objective (RPO) of six (6) hours (100% of service capability and data recovered) and Recovery Time Objective (RTO) of twelve (12) hours or three and a half (3.5) working hours (whichever is lesser) to restore to the agreed RPO or better is at Figure 4 showing the process flow for both scenarios. The process is broken down into 4 phases as follows:

T+1hour (or T+20mins for security incidents)
T+6 hours
T+12 hours
Business as usual.

[Redacted]

Figure 4: Disaster Recovery TimeLine **[Redacted]**

Security Incident Reporting

Where a reported incident relates to Security the MIM will inform the authority within 20 minutes of occurrence.

T + 1 Hour

Once the report is received the MIM will carry out an initial assessment in conjunction with BAS and will:

- Assign additional technical resource as required.
- Manage the Communications requirements

T + 6 Hours

The MIM, in consultation with the sub-contractor BAS will:

- Restore Service via the the Contractor warm back up. This will include the following activities:
  - Repointing of URLs
  - Monitoring of user re-login rates
  - Monitoring system performance
  - Invoke BAS recovery service
  - BAS initiate restore of data from media

T+12 Hours

The MIM in consultation with the sub-contractor BAS will:

- Restore DES AIMS to primary when KDC service is fully restored by:
  - Off-loading all users from active the Contractor warm backup service
  - Initiating resynchronisation of data and application configurations from the active the Contractor warm backup service to KDC Primary
  - Load Backup data sets from media if data resynchronisation fails
  - Re-point all URLs to KDC Primary
  - Notify Users of service availability

T + 13 Hours - Business as usual.

Recovery of Server Services (if not already restored)

Both KDC and the Contractor have access to the ALI, which provides flexibility and resilience for using either location to host OS applications and services.

7.6 Communications

During a BCDR event the MIM is to maintain communications with Authorised Users and key stakeholders. It is anticipated the Authority will use a cascade mechanism to communicate further within their own organisation. The following methods of communication will be used:

- **E-mail notification** - Nominated DE&S PoCs will be notified by email within one hour of the incident, through e-mail distribution groups provided by the Authority and maintained as supporting documentation to the BCDR Plan. An Initial Notification of an incident will be followed by regular Update Notifications, if required, and a Final Notification to inform of a resolution and a return to normal service.

- **On-line notification** - An Initial Notification of an incident will be posted on the on-line DES AIMS Support Facility (if still available), along with regular updates as to the status of the incident. A Final Notification will be posted when a resolution has been implemented and normal service has been resumed.

8 Maintenance, Review and Amendment

The BCDR Plan is maintained, regularly reviewed and updated The Plan and its supporting documents are stored in several secure locations, so they can be easily retrieved and put into practice. Updated BCDR Plans will be made available to the Authority on request.

8.1 BCDR Simulation

A minimum of two successful BCDR simulations will be carried out each year against the required Recovery Point Objective (RPO) of six hours (100% of service capability and data recovered) and Recovery Time Objective (RTO) of twelve hours or three and a half working hours (whichever is lesser) to restore to the agreed RPO or better. These simulations will be closely co-ordinated with the Contractor's sub-contractor BAS and the Authority, and will be conducted utilising a 'warm' standby installation based at the Contractor' site so that the operation of the 'Live' DES AIMS environment is not affected. Following each simulation, a full report will be delivered to the Authority.

8.2 BCDR Review Process

The Contractor will review the BCDR Plan on a quarterly basis, or as requested by the Authority, to ensure that Ensure the Business Continuity Plan and its component parts continue to comply with ISO 27001:2013 and ISO 9001:2015 and MOD Policy.

Each review of the BCDR Plan will include an assessment of the principles and processes set out in the BCDR Plan and any changes in Industry best practices. This will take into account any occurrence or any event since the last review and any changes to the risk to the availability of the DES AIMS. The review will, inter-alia, include the following elements:

- A Review of the Restoration Plans, to determine if sufficient resources are in place to support operations.
- Updating the contact details in the plan, as required.

A review report will be delivered to the Authority within 20 Working Days of the conclusion of each review of the BCDR Plan.

Schedule 13 – Additional Tasking Process

1. BACKGROUND

1.1 This Schedule sets out the procedure for ordering Additional Services as per Schedule 2.

1.2 The Contractor shall not commence the carrying out of any Additional Services without obtaining the prior consent of the Authority in accordance with this Schedule. If the Contractor fails to obtain such consent the Contractor shall have no recourse against the Authority in respect of any costs or liabilities incurred.

2. TASK ORDER

2.1 The Authority may request Additional Services by issuing an additional task order form to the Contractor as set out in Annex A to this Schedule. The Contractor shall within five (5) business days of receipt of the additional task order form, complete Parts 3 and 4 of Annex A to this Schedule and return it to the Authority.

2.3 The Authority shall as soon as reasonably practicable do one of the following:

2.3.1 authorise the additional task order form by completing Part 5 of the relevant additional task order form and returning the form to the Contractor;

2.3.2 in its absolute discretion reject the additional task, in which case it shall notify the Contractor of the rejection; or

2.3.3 require the Contractor to modify Parts 3 and / or 4 of the additional task order form in which case the Contractor shall make such modifications and provide the Authority with an updated additional task order form within such period specified by the Authority or if no period is specified, within five (5) Business Days of such request (in which case the Authority shall have the rights set out in this paragraph 2 in relation to the updated additional task order form.

2.4 The Payment of the additional services received shall be made to the Contractor in accordance with the Part 4 of the additional task order form.

3. COSTS

3.1 Unless expressly agreed otherwise by the Authority in writing in relation to a particular additional service, the Contractor shall be responsible for its own costs and expenses incurred in the preparation and assessment of any additional task order form.

Annex A to Schedule 13 – Tasking Order Form to CCDT/491

Part 1: Requirement [completed by the Authority]

TASK ID: **DATE RAISED:**	**TASK NAME:** **SKILLS EXPECTED:**
EXPECTED OUTPUT (outline): **OUTPUT DELIVERY DATE:**	
DESCRIPTION:	

Part 2: Statement of Work [completed by the Authority]

SERIAL	OUTPUT DESCRIPTION	Outcome	CRITICAL ACCEPTANCE CRITERIA
(add more lines as required)			

Part 3: Proposal for Delivery including breakdown of costs on the basis of the Rate Card at Annex B of Schedule 13 [completed by the Contractor]

Part 4 – Additional Task Milestone payment plan [completed by the Contractor]

Additional Task Milestones	Delivery Date	Amount £ excl. VAT	Acceptance Criteria
Expenses T&S (maximum) supported by receipts, travel expenses allowable from usual place of residence to MoD, Bristol Abbey Wood or other work site as approved by MoD DE&S.			Supported by receipts

Part 5. Authorisation [completed by Authority once Part 3 and 4 have been accepted by the Authority]

AUTHORITY CIO AUTHORISATION	**NAME** **TITLE** **DATE**
AUTHORITY COMMERCIAL AUTHORISATION	**NAME** **TITLE** **DATE**

Annex B Schedule 13 – Rate Card for Additional Services [Redacted]

Day Rate in UK£ against each level and activity

Taken from ITT response:

Level / Scope	Interface and Data Uploading Services	Configuration Services	Training Services including face-to-face and tailored training materials	Data Migration Services	Data Archiving Services	Technical Subject Matter Expertise	MoD Data Processing Activities
1. Follow	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
2. Assist	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
3. Apply	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
4. Enable	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
5. Ensure/Advise	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
6. Initiate/Influence	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
7. Set Strategy/Inspire	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
8. Maximum Travel and Subsistence per day	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Travel and Subsistence (T&S) – The day rates should not include T&S. T&S expenses will be based on a maximum day rate against a Limit of Liability. All T&S costs shall be on a reimbursement basis upon the Contractor providing valid receipts up to the limits specified in the Authority's policy document "Ministry of Defence – Statement of Civilian Personnel Policy – Business Travel Guide V2.0-2017" (to be made available).

Consultant's Working Day – expected to be 8 hours exclusive of travel and lunch. Working Week – Monday to Friday excluding national holidays

Office Hours - 09:00 – 17:00 Monday to Friday - Travel and Subsistence including motor mileage rate.

Annex C to Schedule 13 – Additional Skill Levels Defined

Level	Autonomy	Influence	Complexity	Business Skills
1 Follow	Works under close supervision. Uses little discretion. Is expected to seek guidance in expected situations.	Interacts with immediate colleagues.	Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems.	Uses basic information systems and technology functions, applications, and processes. Demonstrates an organised approach to work. Learns new skills and applies newly acquired knowledge. Has basic oral and written communication skills. Contributes to identifying own development opportunities.
2 Assist	Works under routine supervision. Uses minor discretion in resolving problems or enquiries. Works without frequent reference to others.	Interacts with and may influence immediate colleagues. May have some external contact with Authority's and Contractors. May have more influence in own domain.	Performs a range of varied work activities in a variety of structured environments.	Understands and uses appropriate methods, tools and applications. Demonstrates a rational and organised approach to work. Is aware of health and safety issues. Identifies and negotiates own development opportunities. Has sufficient communication skills for effective dialogue with colleagues. Is able to work in a team. Is able to plan, schedule and monitor own work within short time horizons. Absorbs technical information when it is presented systematically and applies it effectively.
3 Apply	Works under general supervision. Uses discretion in identifying and resolving complex problems and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level.	Interacts with and influences department/project team members. May have working level contact with Authority's and Contractors. In predictable and structured areas may supervise others. Makes decisions which may impact on the work assigned to individuals or phases of projects.	Performs a broad range of work, sometimes complex and non-routine, in a variety of environments.	Understands and uses appropriate methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Takes the initiative in identifying and negotiating appropriate development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation and procedures. Absorbs and applies technical information. Works to required standards. Understands and uses appropriate methods, tools and applications. Appreciates the wider field of information systems, and how own role relates to other roles

				and to the business of the employer or client.
4 Enable	Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes.	Influences team and specialist peers internally. Influences Authority's at account level and Contractors. Has some responsibility for the work of others and for the allocation of resources. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives.	Performs a broad range of complex technical or professional work activities, in a variety of contexts.	Selects appropriately from applicable standards, methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Communicates fluently orally and in writing, and can present complex technical information to both technical and non-technical audiences. Facilitates collaboration between stakeholders who share common objectives. Plans, schedules and monitors work to meet time and quality targets and in accordance with relevant legislation and procedures. Rapidly absorbs new technical information and applies it effectively. Has a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client. Maintains an awareness of developing technologies and their application and takes some responsibility for personal development.
5 Ensure /Advise	Works under broad direction. Is fully accountable for own technical work and/or project/ supervisory responsibilities. Receives assignments in the form of objectives. Establishes own milestones and team objectives, and delegates responsibilities. Work is often self-initiated.	Influences organisation, customers, contractors and peers within industry on the contribution of own specialism. Has significant responsibility for the work of others and for the allocation of resources. Makes decisions which impact on the success of assigned projects i.e. results, deadlines and budget. Develops business relationships with the Authority.	Performs a challenging range and variety of complex technical or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/ organisational requirements.	Advises on the available standards, methods, tools and applications relevant to own specialism and can make correct choices from alternatives. Analyses, diagnoses, designs, plans, execute and evaluates work to time, cost and quality targets. Communicates effectively, formally and informally, with colleagues, subordinates and customers. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Understands the relevance of own area of responsibility/ specialism to the employing organisation. Takes customer requirements into account when making proposals. Takes initiative to keep skills up to date. Mentors more junior colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for operational improvement. Demonstrates creativity and innovation in applying solutions for the benefit of

				the Authority.
6 Initiate/ Influence	Has defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and delegates responsibilities. Is accountable for actions and decisions taken by self and subordinates.	Influences policy formation on the contribution of own specialism to business objectives. Influences a significant part of own organisation and influences the Authority/contractors and industry at senior management level. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance. Develops high-level relationships with the Authority, contractors and industry leaders.	Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the formulation of IT strategy. Creatively applies a wide range of technical and/or management principles.	Absorbs complex technical information and communicates effectively at all levels to both technical and non-technical audiences. Assesses and evaluates risk. Understands the implications of new technologies. Demonstrates clear leadership and the ability to influence and persuade. Has a broad understanding of all aspects of IT and deep understanding of own specialism(s). Understands and communicates the role and impact of IT in the employing organisation and promotes compliance with relevant legislation. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry.
7 Set Strategy/ Inspire	Has authority and responsibility for all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made, both by self and subordinates	Makes decisions critical to organisational success. Influences developments within the IT industry at the highest levels. Advances the knowledge and/or exploitation of IT within one or more organisations. Develops long-term strategic relationships with customers and industry leaders.	Leads on the formulation and application of strategy. Applies the highest level of management and leadership skills. Has a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment	Has a full range of strategic management and leadership skills. Understands, explains and presents complex technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. Has a broad and deep IT knowledge coupled with equivalent knowledge of the activities of those businesses and other organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies. Assesses the impact of legislation, and actively promotes compliance. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in IT in own area(s) of expertise.

Schedule 14 – Not used

Schedule 15 – User Access Control

1 Introduction

Authorised Users for DES AIMS will be spread across a number of MOD and Industry Partner organisations covering 26 Air Systems and located across 17 geographical locations. Authorised Users will require access to differing elements of the processes and will need controlled access to the data relevant to their area of work.

DES AIMS will provide the ability to configure each Authorised User's access control and permissions across all the DES AIMS business processes. This includes a comprehensive set of Roles, ensuring that Users are able to complete airworthiness tasks effectively and within the constraints of their delegated authority. Taut Access Control in a highly regulated and complex Military Aviation Environment is essential to deliver safe and airworthy operations. This is fully allied with the embedded Process and Workflow System component, enabling digital signatures at each appropriate stage.

2 Authorised User Types

Authorised Users can be granted access to one or more Air Systems and are grouped into the following user types (User Types taken from the 'DES AIMS Data Access Strategy' document included within the Dataroom for the ITT):

- **Front Line Command (FLC) User** – These Users will generally be based with the Air Systems undertaking maintenance and related roles.
- **Industry Partner User –** These Users are based in the Industry Partners responsible for delivering the Air Systems to the MOD. They will be heavily linked to Delivery Teams (DT) and specific Air Systems which they have delivered and may be based at their own sites, with FLC Users or at DE&S locations.
- **DE&S DT User –** These Users are responsible for monitoring the Air Systems and ensuring their continued Airworthiness. They provide the link between the FLCs and Industry Partners.
- **DE&S Senior User (i.e. TAA) –** These Users are the senior staff responsible and accountable for the Airworthiness of Air Systems.

3 Authorised User Accounts

In order to maintain the appropriate level of control of the airworthiness data contained in DES AIMS, a formal application for access must be completed for each user. This application is made on an Authorised User Application Form configured for DES AIMS. The form will be processed electronically, guiding the User through the application steps and allowing the appropriate approval to be recorded by the Authority's nominated representative(s). On completion, the System Administrator uses the DES AIMS 'Access Control Account Management' interface to create the appropriate Authorised User account. Access is via a unique user-name and password combination and the Authorisation is attached to the User record.

Each Authorised User's account requires a full name and assigned Post. The Post name relates to the post the user holds within their own organisation (e.g. EA Ground Systems) and this is assigned the appropriate number of approved DES AIMS Roles. Multiple Roles can be assigned providing access to several Air Systems and/or allowing the User to undertake a variety of tasks within each Air System. Each Role carries permissions or capabilities to

access, complete and progress issues/entities. An individual Authorised User account is created when the name, post and role(s) are linked. The account is then enabled and the User is advised. Authorised Users access the DES AIMS via a single portal with Single-Sign-On capability. Once enabled Users are allowed to update contact details and passwords themselves via the Online Portal.

4 Adding and Amending Authorised Users

The Authority provides written confirmation of any Authorised User accounts that need to be added or amended. Amendment includes the addition or revocation of existing Roles. This written confirmation is stored with the record to ensure traceability and in accordance with ISO27001 best practice. Addition/amendment of accounts is completed by the Contractor in the timescales identified in the System Administration SLA (Annex B to Schedule 11).

5 Removing/Disabling Authorised Users

The Authority is required to notify the System Administrator of any Authorised User accounts that need to be removed or temporarily disabled. Routine notification of required removals will be provided monthly but removals can be requested immediately in the case of a security concern. Removal requests must list as a minimum: Post Title and user name and must be approved by an authorised person. Removal of such accounts will be completed in the timescales identified in the System Administration SLA (Annex B to Schedule 11). Removal or deactivation of an account prevents all further access to DES AIMS by the User, however the account holder's post will continue to be allocated to the actions/activities assigned to them until these are inherited by an alternative user. Accounts cannot be fully deleted as they are part of the ISO27001 and BS10008 audit record.

6 Scaling the Service

The DES AIMS solution is scalable up or down to match the number of Authorised User accounts required by the Authority. For planning purposes the Authority is requested to supply quarterly a forecast of the variation of the number of Authorised Users in increments of 50.

7 Authority System Administration Activity

The Authority has identified an option to take over the System Administration Support services over the life of the DES AIMS service. The Authority will be able to manage the four Authorised User Types including adding, amending or removing/disabling of accounts.

7.1 Role and Capability Changes

As the Roles available are created as part of the process design then a System Administrator has no facility to create new DES AIMS Roles. Creation of a new role would need to be analysed and implemented by the Contractor and the System Administration Console updated accordingly. It should also be noted that some post identifier changes or post transfers maybe outside the scope of the System Administrator for data integrity and audit trail purposes.

Schedule 16 – Security Aspects Letter

Ministry of Defence

de&s

Nick Hillier-Smith
DES CIO

030 679 89932

nick.hillier-smith855@mod.gov.uk

Defence Equipment & Support
Elm 2c, #4139
MOD Abbey Wood
Bristol BS34 8JH

FAO: TLM Nexus

11-Feb-19 Our Reference:

AIRWORTHINESS ISSUES MANAGEMENT SYSTEM (AIMS) SECURITY ASPECTS LETTER

Messrs .....

For the personal attention of: (Name of company Security Controller)

Dear Sir

TENDER NO AND SUBJECT: CCDT/491 AIRWORTHINESS ISSUES MANAGEMENT SYSTEM

1. On behalf of the Secretary of State for Defence, I hereby give you notice that any sketch, model, article, note or document, or information connected with or arising out of the above-mentioned Invitation to Tender, is subject to the provisions of the Official Secrets Acts (OSA) 1911-1989. Your attention is particularly drawn to the following specific classified aspects which must be fully safeguarded:

SECURITY ASPECTS	CLASSIFICATION
Air System name	Unclassified
Air System technical details	up to Official-Sensitive
Air System 'Issue' details	up to Official-Sensitive
Air System Hazard details	up to Official-Sensitive
Data imported from other air environment tools	up to Official-Sensitive

4. Will you please confirm that:

a. This definition of the classified aspects of the above Invitation to Tender has been brought to the attention of the person directly responsible for the security of this Tender.

b. The definition is fully understood.

c. Measures can, and will, be taken to safeguard the classified aspects.

d**.** All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information associated with this contract.

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. In the event of a contract being placed with you, these aspects would constitute `SECRET Matter' for the purpose of the Security Clause included in the contract and as OFFICIAL-SENSITIVE.

7. Any access to classified information on MoD premises that may be needed will be subject to MoD security regulations under the direction of the MoD Project Officer.

Yours faithfully

Copy via DII email to:

DES PSyA-SecurityAdviceCentre (MULTIUSER)
DSR-STInd (MULTIUSER)
ISS Des-DAIS-SRAAcc8-IA (Collins, David C1))

Approved for release:

Andy Read
Air Cdre
AIMS Senior Responsible Owner (SRO)