Strategic Command
Defence Support

Statement of Work

Application Hosting

V0.1

Author

Rob Austen, SolArch1

Annex A

G-Cloud-12

PAGE INTENTIONALLY BLANK

Table of Contents

Configuration History

TITLE:	**Statement of Work Application Hosting**		
Date:	14 Feb 22	**Release:**	0.4
Author:	Rob Austen, UKStratCom-DefSp-WG-DA-SolArch1		
Owner:	WG DA		

Revision History

Revision Date	Summary and nature of changes	Version
26 Oct 21	Initial Draft	0.1
29 Oct 21	Update post initial internal review	0.2
24 Jan 22	Internal Review	0.3
14 Feb 22	Clarification Questions	0.4

Approvals

This document requires the following approvals:

Name	Signature	Appointment	Date	Version

Distribution

This document has been distributed to the following for information only:

Name	Title	Date of Issue	Version

Glossary of Terms

Term	Definition
ASSC	Assets Subject to Special Control
CCMIS	Customs and Compliance Management Information System
CyDR	Cyber Defence and Risk
DR	Disaster Recovery
HMG	Her Majesties Government
HMRC	Her Majesties Revenue and Customs
HVAC	Heating, Ventilation and Air Conditioning
IMM	Integrated Movements Management
ISO	International Standards Organisation
ITHC	Information Technology Health Check
ITV	In-Transit Visibility
LAN	Local Area Network
MCN	MOD Core Network
MOD	Ministry of Defence
OGD	Other Government Departments
OS	Operating System
OSD	Out of Service Date
PaaS	Platform as a Service
RAMP	Remote Access Movements Portal
RHEL	Red Hat Enterprise Linux
RLI	Restricted LAN Interconnect
RMADS	Risk Management and Accreditation Documentation Set
SAC	Security Assurance Coordinator
SC	Security Check
SLA	Service Level Agreement
SMI	Secure Managed Interface
SOW	Statement of Work
SWG	Security Working Group
UII	Unique Item Identification
UK	United Kingdom
US DoT	United States Department of Transportation
WG	WATERGUARD
WG Apps	WATERGUARD Applications

Hosting and Infrastructure Support

Background

1. The WG Programme is currently responsible for the delivery of two applications into the Defence Portfolio: RAMP and WG Apps. Both are web-based applications accredited to hold information up to and including OFFICIAL-SENSITIVE and are accessed by members of the MOD, Industry and Other Government Departments (OGD) over the MOD Core Network (MCN) and over the Internet.

Platform as a Service

2. The hosting and infrastructure support for RAMP and for WG Apps will be provided through a 'Platform as a Service' (PaaS) offering. The PaaS will provide secure, United Kingdom (UK)-based, Private Cloud infrastructure that can provide hosting and enable the sharing OFFICIAL-SENSITIVE information between the MOD and Stakeholders. The infrastructure must provide Internet and Restricted LAN Interconnect (RLI)/ Secure Managed Interface (SMI) connectivity and be accredited by Cyber Defence and Risk (CyDR).

3. Key features characterising the PaaS requirement for RAMP and WG Apps are outlined below:

a. The PaaS must be hosted in a Secure UK Data Centre and managed by staff with a minimum Security Clearance of Security Check (SC).

b. The PaaS must be accredited by the MOD to hold information up to and including OFFICIAL-SENSITIVE.

c. The PaaS must have connectivity to the RLI/SMI, and to the Internet.

d. The PaaS must be able to provide 24/7/365 availability.

e. The PaaS must support applications running on Windows Server 2016 and Red Hat Enterprise Linux (RHEL) 7.

4. The distinction between boundaries of support, that defines what is meant by PaaS is detailed in Figure 1 below.

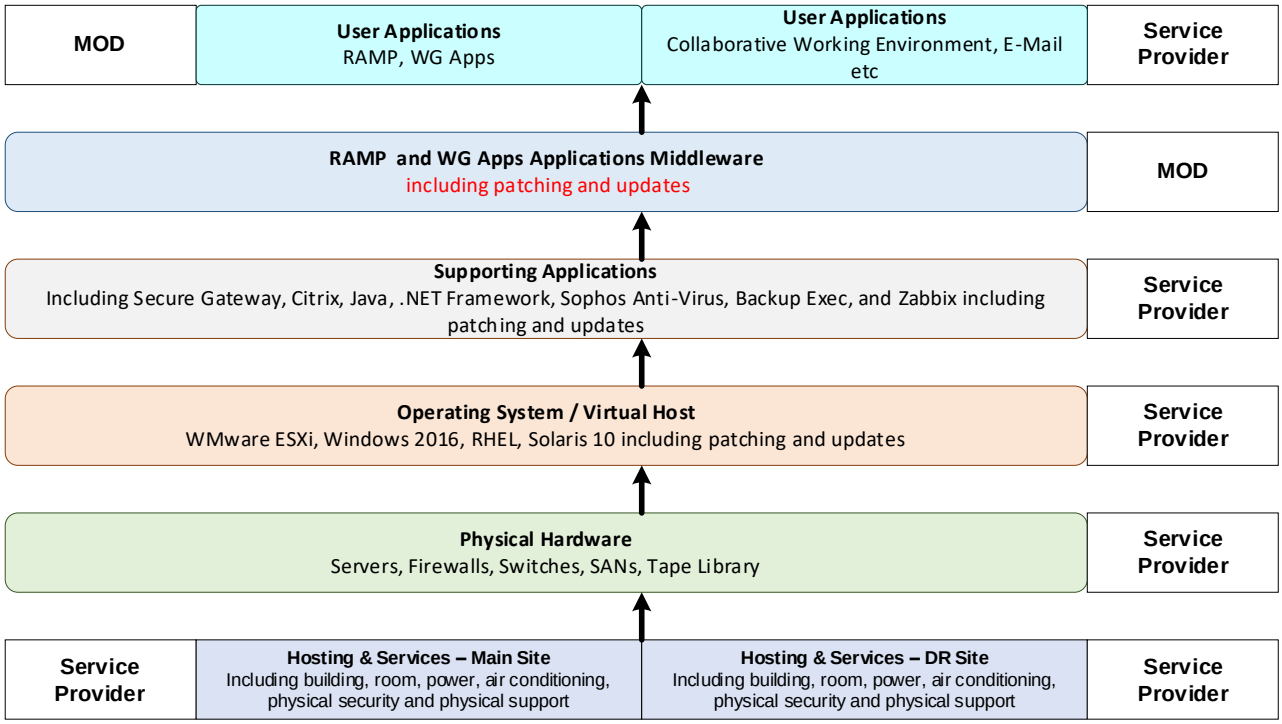

Figure 1 - Support Boundaries

In-Scope

5. The following services must be included within the provision of the PaaS:

Primary Site

a. Data Centre.

b. Communications:

(1) Internet Provision.

(2) RLI Provision.

(3) Disaster Recovery (DR) Site Link.

c. Hardware:

(1) Secure Gateways (Internet and RLI).

(2) Network Infrastructure directly associated with the provision of RAMP and WG Apps.

(3) Monitoring Infrastructure directly associated with the provision of RAMP and WG Apps.

(4) A Cloud Environment.

(5) Hardware directly associated with the hosting of RAMP and WG Apps.

(6) Backup Servers and Storage (including Tape Library) directly associated with the provision of RAMP and WG Apps.

d. Software:

(1) VMWare Virtualisation.

(2) Host Operating Systems.

(3) Virtual Machine Operating Systems including Operating System (OS) Patching (Windows Server 2016 and Red Hat Enterprise Linux (RHEL).

(4) Disaster Recovery Software.

(5) All relevant equipment firmware.

Disaster Recovery Site

e. Data Centre.

f. Communications:

(1) Internet Provision.

(2) RLI Provision.

(3) DR Site Link.

g. Hardware:

(1) Secure Gateways (Internet and RLI).

(2) Network Infrastructure directly associated with RAMP and WG Apps provision.

(3) Monitoring Infrastructure directly associated with RAMP and WG Apps provision.

(4) A Cloud Environment.

(5) Hardware directly associated with the hosting of RAMP and WG Apps.

(6) Backup Servers and Storage (including Tape Library) directly associated with the provision of RAMP and WG Apps.

Out of Scope

6. This statement of Requirement specifically excludes:

a. Any client code supplied by the Authority or one of their suppliers for which the Hosting Provider is not considered responsible.

b. Hosting and support of the Secure Managed Interconnect 2 (SMI-2) Gateway, provision of which is an Authority responsibility.

c. Hosting and support of the Restricted LAN Interconnect, provision of which is an Authority responsibility.

Service Support

Support Hours

7. Table 1 defines how Support Hours are defined in this document.

Support Hours Period	**Period Covered**
Core Hours	08:00 to 18:00 Monday to Friday excluding Bank Holidays in England
Operating Hours	00:00 to 23:59 Daily

Table 1 - Support Hours

8. Table 2 defines the requirement for the provision of support services.

Service Area	**Support Hours Period Provided Within**
All Services	Core Hours
Service Desk	Core Hours
Services for Critical level severity Support Requirement	Core Hours
Monitoring Services	Core Hours
Agreed change control process managed changes (at least 5 days working notice will be provided)	Core Hours or Out of Hours for changes that require a service outage

Table 2 - Support and Maintenance Services

Service Desk

9. The provision of a Service Desk, accessible via Telephone or e-mail, to provide technical support to authorised Authority personnel using, maintaining or amending the RAMP or WG Apps applications.

10. Service Desk support should include, but not be limited to:

a. Logging Support Requirements, obtaining any further information required by the Hosting Provider in order to resolve Support Requirements and keeping the Client updated regarding the status of Support Requirements;

b. Answering queries on the use and operation of the System;

c. Answering queries on System documentation;

d. Guidance in operation of the System;

e. Assistance in identifying and verifying the causes of suspected Incidents in the System; and

f. Advice on bypassing or mitigating identified Incidents in the System.

Service Level Timescales

11. Table 3 details the service levels and response times that the Authority would desire to see the service operate under.

Severity Level	Description	Response Time	Update Frequency	Resolution Agreed
Critical	Entire solution is unavailable / full services are down for any period	15 min	30 min	4 hours
High	Operation of service is degraded, or major services are not functional	60 min	60 min	8 hours
Normal	Errors that are non-disabling or cosmetic and clearly have little or minor impact on the normal operation of the services	4 hours	24 hours	Not Applicable

Table 3 - Service Response Times

12. In measuring response times it is accepted that:

a. All response times will be calculated from Support Requirement commencement;

b. All response times will only be considered applicable to Support Requirements raised through a phone call from the Client or a ticket raised by the Client where the Client has correctly classified the severity level of the Support Requirement;

c. Resolution agreed only applies to Support Requirements where the root cause falls within the Hosting Solution providers responsibility; and

d. The Resolution agreed is satisfied when the Support Requirement is either resolved, or a time frame and plan for full resolution has been communicated to the Client.

13. The Client can be expected to provide the Hosting Service provider with accurate and prompt notification of any problem and assist the Hosting Service provider as may reasonably be required to diagnose problems and implement any resolution agreed.

Availability

14. The Availability of the System in any month should be at least 98%

15. Availability for a month shall be calculated following the end of that month using the formula:

$$\text{“Availability”} = \frac{(OH - D)}{OH} \times 100$$

16. Where:

a. OH = Total Operating Hours of the System during the month

b. D = Total Downtime during Operating Hours during the month, where “Downtime” means non-availability of one or more of the primary functions of the System (as set out in the Specifications) but excludes any downtime that is:

(1) pre-agreed with the authority;

(2) due to emergency or scheduled maintenance;

(3) due to failover in a disaster recovery scenario;

(4) attributable to the Client or its Client’s actions or omissions;

(5) due to issues in Client’s data integrity, system software, the operating system, vendor supplied patches and/or application code;

(6) due to application load and/or traffic spikes;

(7) caused by an application operated by the Client on its system;

(8) attributable to a HMG network beyond the UKFast network boundary;

(9) caused by capacity management for which the Client is responsible; and

(10) caused by the Client’s failure to respond to an alert from the Hosting Providers monitoring tool.

Accreditation

17. RAMP and WG Apps are both fully accredited by the MOD to hold information up to and including OFFICIAL-SENSITIVE. Accreditation for the applications does not include, but is dependent upon, the accreditation of the underlying hosting environment.

18. The boundary of responsibility for Application and Hosting Environment accreditation is illustrated in Figure 2 below.

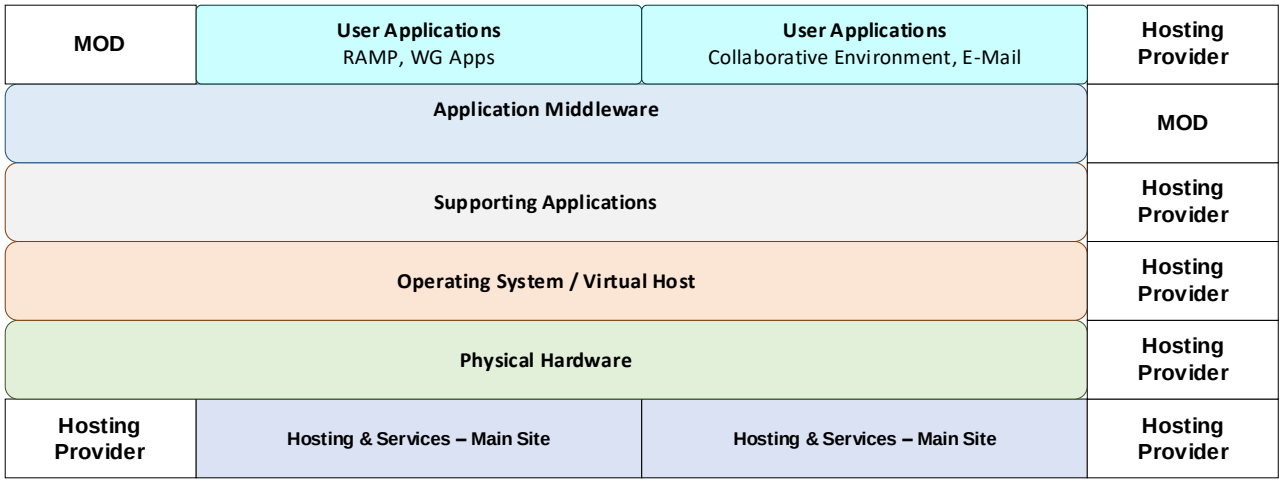

Figure 2 - Accreditation Responsibility Scope

Remote Access Movements Portal

Background

19. The business aims and objectives supported by RAMP are two-fold:

    a. To provide an Integrated Movements Management (IMM) capability that will support the delivery of an integrated cargo booking, and the allocation and manifesting of freight for all modes of movement, surface or air, commercial or military. The IMM capability can be integrated with industry partners and OGD, including Her Majesty's Revenue and Customs (HMRC) and the United Kingdom (UK) Border Force, to support the efficient and effective prosecution of defence movements globally.

    b. To provide In-Transit Visibility (ITV) functionality that will support the delivery of an integrated capability to determine, and visualise where necessary, the location and status of defence inventory and assets whilst in-transit through the Defence Support Chain. Information is provided to appropriate degrees of accuracy and timeliness, thereby supporting efficient and effective resource management, and enabling effective decision making.

20. RAMP is a web-based application that is accessible to MOD personnel, and to approved Industry Contractors and Other Government Departments (OGD). The application is developed as a joint venture between the MOD and the United States (US) Department of Transportation (DoT) – Volpe[1] and has been in use within the MOD since 2009.

21. Originally hosted in the US, RAMP was re-hosted into the United Kingdom (UK) in 2019 to address a Risk Balance Case associated with the off shoring of MOD information.

Application Details

22. There are 6 instances of the RAMP Environment:

    a. Production;

[1] Volpe is the name given to the element of the DoT working out of the Volpe Centre, Boston MA.

b. Pre-production;

c. Training;

d. QA;

e. Development; and,

f. Disaster Recovery.

23. All environments are built using the same technology stack as illustrated in Figure 3 below.

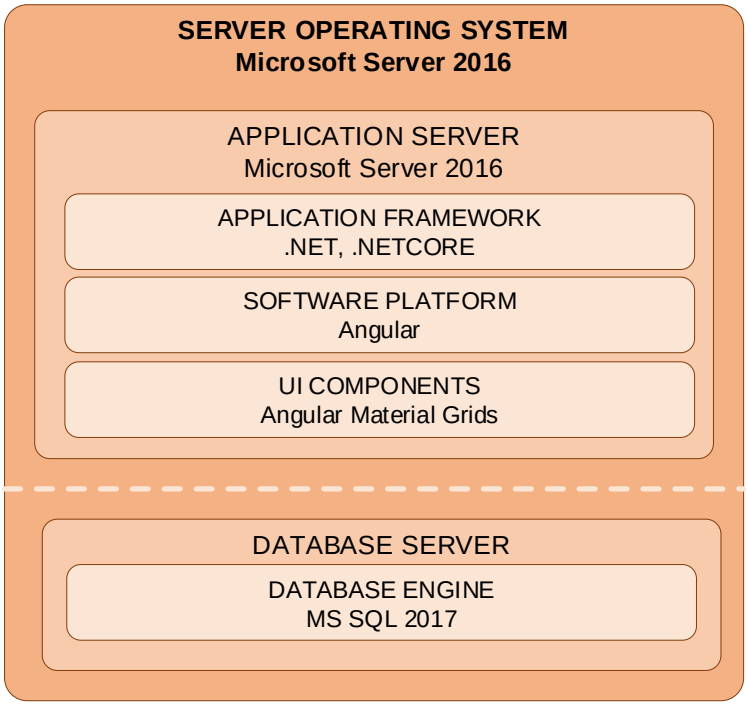

Figure 3 - Application Design

WATERGUARD Applications

24. The business aims and objectives supported by WG Apps are:

a. To support the MOD in maintaining compliance with HMRC regulatory requirements for the import and export of materiel and equipment;

b. To implement a capability to manage information relating to Assets Subject to Special Controls (ASSC);

c. To maintain a master record of all instances of Unique Item Identification (UII) marks being used within the MOD, as well as supporting the marking of assets and equipment by the MOD and its contractors; and

d. To enable the MOD to properly manage the Out of Service Dates (OSD) of its platforms and equipment and, through this, to ensure that the deprecation of fixed assets and capital spares is accurate.

25. WG Apps is a web-based application that is accessible to MOD personnel, and to approved Industry Contractors and OGD. The application requires access over the MOD Core Network and via the Internet.

Application Details

26. There are 9 instances of the WG Apps environment:

a. Customs and Compliance Management Information System (CCMIS) Production;

b. CCMIS Pre-Production;

c. CCMIS Test;

d. CCMIS DR;

e. ASSC Registry (ASSC-Reg) Production;

f. ASSC-Reg Pre-production;

g. ASSC-Reg Test;

h. ASSC-Reg Training[2]; and

i. ASSC-Reg DR.

27. All environments are built using the same technology stack as illustrated in Figure 4 below.

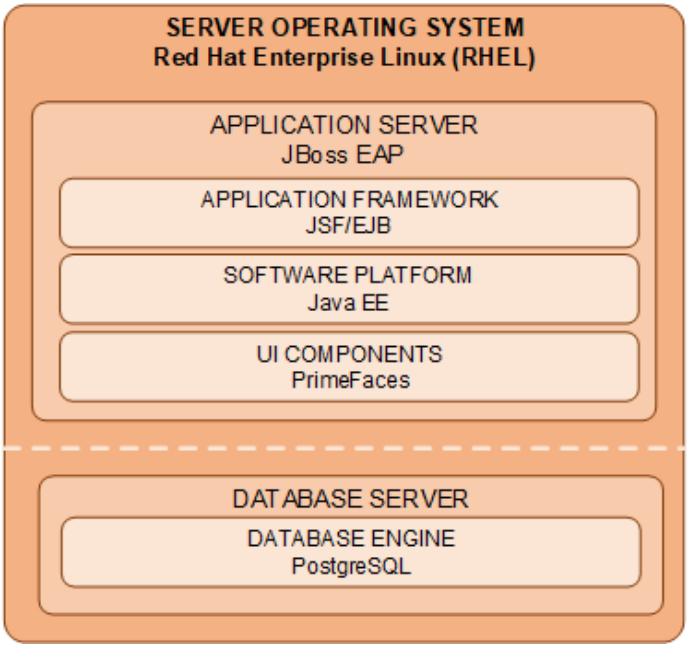

Figure 4 - Application Design

[2] Previously known as ASSC-Reg "EX-TEST"

Statement of Work

28. This Statement of work covers the period 01 Apr 22 to 31 Mar 23 and will be reviewed/renewed annually.

29. Table *4* below articulates the WATERGUARD Application Hosting SOW:

Task ID	Work Item	Criticality K – Key	Acceptance Criteria	Validation Method
1. Support and Maintenance Services				
1.1	**Foundation Service** The Hosting Provider will provide functioning Hardware required to run the RAMP and WG Apps environments and manage the physical hosting within a data centre	K	All data must be hosted within the UK Access to the data centre must be security controlled	Initial User Acceptance
1.2	**Operating System Management** Install and provide basic configuration and support of application software purchased through The Hosting Provider as part of the Client Solution	K	User Verification of initial installation Operating System (OS) Patching to be carried out on an automated schedule with restarts agreed for a pre-defined time outside of normal operating hours Critical Security Patches to be applied within 7 working days following testing	Initial User Acceptance Monthly Reports Quarterly Review Meetings
	Firewall Management Install and maintain the configuration of a Hardware firewall.	K	Configuration requests to be completed in accordance with the Service Levels defined in this SoW.	Monthly Reports Quarterly Review Meetings

	Business Continuity. 1. Perform Daily Backup of the RAMP and WG Apps Environments 2. Ensure Availability Criteria of the Service can be maintained 3. Restore service to a known point in the event of a full system failure		Identify, correct, and use reasonable endeavours to re-run failed backup issues within 8 core hours Platform meets availability Targets demonstrated through Monthly Report	Monthly Reports Quarterly Review Meetings
	Anti-virus Management will install and maintain anti-virus software	K	Must meet the minimum requirements for Data Centre and Application accreditation	Initial Acceptance Monthly Reports Quarterly Review Meetings
	Monitoring and Alert Management Provide system health monitoring for all server hardware and provide pro-active investigation of received alerts.	K	Alerts should include, but not be limited to: • Unexpected Server Restarts • Free Disk Space (20%, 10%, 5%, 1% remaining)	Monthly Reports Quarterly Review Meetings
	Application Installation and Configuration Provide the initial installation and maintain agreed configuration of foundation applications. RAMP and WG Apps and their associated middleware are specifically excluded from this requirement as patching of		Provide patching of agreed applications	Monthly Reports Quarterly Review Meetings

	these applications will be undertaken by a 3rd party.			
	Quality Management The Hosting Provider should maintain certification for: 1. ISO9001 (Quality Management System) 2. ISO14001 (Environmental Management Systems) 3. ISO20000 (Service Management Systems) 4. ISO/IWC27001 (Information Security Management Systems)		Copies of Certificates.	Demonstration
	Capacity and Availability Management Provide concurrent flexible access to the services to a user base that can grow, over the period of performance of the contract		No system outages caused as a result of adding users to the system No system outages as a result of concurrent use of the system by authorised users Platform available from 00:00 to 23:59 daily Platform to meet a 98% Availability rate	Monthly Report Quarterly Review Meetings
	Service Desk Support 1. 1st Line Support Desk 2. 2nd Line Application Support 3. Account Creation/Archive		Availability against Core Hours Reported in Monthly Report	Monthly Report Quarterly Review Meetings

	4. Password Reset			
2. Accreditation				
2.1	**<u>Hosting Environment Accreditation</u>** The Hosting Provider will provide and maintain a hosting environment that is accredited by the MOD to hold data up to and including OFFICIAL-SENSITIVE	K	Copy of Accreditation Certificate for the Hosting Environment Copy of Accreditation Letter for the Hosting Environment	Copy at initial Contract Award Documents to be up-issued at each renewal point for the Platform Accreditation
2.2	**<u>IT Health Check</u>**. 1. The Hosting Provider will arrange for the annual Information Technology Health Check (ITHC) to be undertaken against the RAMP Application. 2. The Hosting Provider will arrange for the annual ITHC to be undertaken against the WG Apps Application	K	Approved Scope of ITHC Acceptance of ITHC Report	Scope to be agreed between the MOD and the ITHC provider Acceptance to be agreed with the MOD Security Assurance Coordinator for WG Apps and for RAMP.
	<u>Security Working Group</u> 1. Provide appropriate representation at the RAMP Security Working Group (SWG) 2. Provide appropriate representation at a WG Apps Security Working Group (SWG)		Attendance (virtual or physical) of appropriately qualified representative at the SWG	It should be anticipated that an SWG will be held for each application at 6-monthly intervals.
	<u>Support to Application Accreditation</u>			

	1. Support the Authority in maintaining accreditation for RAMP 2. Support the Authority in maintaining accreditation for WG Apps		Provision, at the Authority's request, of relevant information about the hosting service to support the provision of Risk Management and Accreditation Documentation Sets (RMADS) for RAMP and WG Apps	Support will be limited to provision of information about the hosting service, not for completion of the RMADS documents themselves
X. Documentation				
	<u>Forensic Readiness Plan</u> A document describing details of the Forensic Readiness and the associated management activities undertaken by the Hosting Provider required to be able to collect, preserve, protect and analyse Digital Evidence so that this evidence can be effectively used in any legal matters, in security investigations, in disciplinary matters, in an employment tribunal or in a court of law.		To be issued within 1 month of Contract Award and up-issued on any significant changes	Document should be approved by the Security Assurance Coordinator (SAC) for RAMP and for WG Apps.
	<u>In-Service Management Plan</u> An In-service Management Plan is required to ensure that the delivery of the service is carried out in a consistent and effective manner. The In-Service Management Plan should be worked up in conjunction with the Service Level Agreement and should include the following: • Event Management		To be issued within 1 month of Contract Award and up-issued on any significant changes	Initial Acceptance Quarterly Review Meetings

	• Incident Management • Problem Management • Change Management • Access Management • Security Management • Knowledge Management			
	Exit Plan In accordance with Clause 21 of the Tasking Order Form. The Exit Plan shall be produced to detail the exit strategy in the event of a termination notice of the contract, or the removal of the requirement for hosting either RAMP or WG Apps from the contract.		To be issued within 1 month of Contract Award and up-issued on any significant changes.	Initial Acceptance Quarterly Review Meetings
	Business Continuity and Disaster Recovery Plan The Business Continuity and Disaster Recovery Plan will provide details of how the Hosting Provider will continue the day-to-day delivery of the RAMP service, the WG Apps Service, the supporting hosting infrastructure, and the internal services, in the event of any degree of disruption or disaster.		To be issued within 1 month of Contract Award and up-issued on any significant changes	Initial Acceptance Quarterly Review Meetings
	Architecture Diagrams The Authority requires a set of architecture diagrams to be created and maintained detailing the High-level architecture of the hosting environments		To be issued within 1 month of Contract Award and up-issued on any significant changes	Initial Acceptance Quarterly Review Meetings

	Asset Register Provision of a document detailing the Hardware and Software assets that form part of the PaaS		To be issued within 1 month of Contract Award and up issued on any significant changes	Initial Acceptance Quarterly Review Meetings
	Environmental Policy Statement The Hosting Provider must provide a copy of their Environmental Policy Statement stating how they will monitor and measure their Carbon Footprint and detailing any specific measures undertaken to address environmental concerns associated with the operation of the PaaS		An Environmental Policy Statement should be issued within 1 month of Contract Award	Authority acceptance of the Environmental Policy Statement
X. Contract Management				
	Monthly Service Reporting The Hosting Provider should provide Monthly Service Management Reports		Report to be issued within 10 days of month-end and should include, but not be limited to: • Service Summary (Active Users by Service, Service Level Agreement (SLA) Targets) • User Details • Service Management (record of Tickets Raised) • Environment Performance	Acceptance of the report. Quarterly Review Meetings

			• Uptime Availability • System Maintenance (Planned and Actual)	
	Quarterly Service Reporting The hosting Provider will support a Quarterly Review Meeting that should discuss, but not be limited to: 1. Contract Performance over the preceding Quarter 2. Capacity and Availability Management 3. Planned Changes to Service (Authority or Provider)	Key	Meeting to be held within 3 weeks of the end of each quarter.	Monthly Review Meetings
	Information Sharing The Hosting Provider shall provide an approved means of sharing information relating to the Hosting Service up to and including OFFICIAL-SENSITIVE		Validation that the proposed solution is accredited to support information sharing up to, and including, OFFICIAL-SENSITIVE.	Initial Acceptance

Table 4 - Application Hosting Statement of Work

Key Performance Indicators

30. The following Key Performance Indicators have been identified for the contract.

Ser	Description	Good	Approaching Target	Requires Improvement	Inadequate
1	System Availability – The availability of the system in any month should be at least 98%	≥ 98%	95-98 %	90-95%	≤ 90%
2	Event Management – Provide a timely and proportionate response to Events based on the Severity Level[3]	Response Time: • Critical ≤ 30 min • High ≤ 1 hr • Normal ≤ 4 hrs Resolution Agreed • Critical ≤ 4 hrs • High ≤ 8 hrs • Normal N/A	Response Time: • Critical ≤ 1 hr • High ≤ 2 hrs • Normal ≤ 6 hrs Resolution Agreed • Critical ≤ 6 hrs • High ≤ 12 hrs • Normal N/A	Response Time: • Critical ≤ 2 hr • High ≤ 4 hrs • Normal ≤ 12 hrs Resolution Agreed • Critical ≤ 12 hrs • High ≤ 16 hrs • Normal N/A	Response Time: • Critical > 2 hr • High > 4 hrs • Normal > 12 hrs Resolution Agreed • Critical > 12 hrs • High > 16 hrs • Normal N/A
3	Data Recovery – Target timeline for data loss recovery (during support hours)	≤ 4 hours	4-5 hours	5-8 hours	≥ 8 hours
4	Contract Management – Production of Monthly Reports	≤ 10 days	10-15 days	15-20 days	≥ 20 days

[3] Severity Levels are: Critical – Entire solution is unavailable / full services are down; High – Operation of service is degraded, or major services are not functional; Normal – Errors that are non-disabling or cosmetic and clearly have little or minor impact on the normal operation of the services.