FUTURE SERVICE DELIVERY CONTRACT

SCHEDULE 2.1

SERVICES DESCRIPTION

PART 21 – TRACEABILITY MATRIX

For each of the Parts of Schedule 2.1 and the other Schedules listed below, the Contractor has completed this Traceability Matrix to indicate where in Schedule 4.1 (Contractor Solution) it has set out how it will meet the relevant Authority Requirement.

Heading/Subject Matter	Paragraph	Requirement	Traceability - Location in Schedule 4.1 (Contractor Solution)
Schedule 2.1, Part 8 (MIL MIT & DATA)			
BAU & SUPPORT {H1–H6} - Providing the Mil Pers & Vets Reporting Platform (MP&VRP): {H1}	2.1	The Contractor acknowledges that this requirement is related to ensuring that the MP&VRP is available, fully functioning, and accurate.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.1 - 1.3.6
BAU & SUPPORT {H1–H6} - Providing the Mil Pers & Vets Reporting Platform (MP&VRP): {H1}	2.2	The Contractor shall: (a) ensure the MP&VRP is fully functional according to the latest agreed version of the Logical Application Model for the underlying application and available in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1); (b) run, extract, transform, and load the initial, full, and incremental Data loads according to the 'Refresh Schedule' (being a document, agreed by the Authority, setting out the frequency at which the Data in the MP&VRP gets updated from the source system(s)) and to meet the structural and business requirements of the Data being loaded, includes differing refresh frequencies for different data sets post-delivery of serial H33 of Annex H to Schedule 2.1; (c) ensure all MP&VRP Data refreshes complete outside of Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1), unless agreed otherwise in writing by the Authority (MilPers MI Mgr); (d) ensure the MP&VRP Data accurately reflects all data sources (as at time of extraction); and	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.1 - 1.3.6

		(e) ensure that any MP&VRP Service Downtime required during Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1) is agreed, in writing, by the Authority (MilPers MI Mgr) prior to such Service Downtime taking place.	
BAU & SUPPORT {H1–H6} - MP&VRP Performance and Improvement {H2}	2.3	The Contractor acknowledges that this requirement is to ensure there is a Contractor culture of continually assessing the MP&VRP and identifying inefficiencies and performance issues, investigating the causes, and proposing and implementing solutions.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.7 - 1.3.11
BAU & SUPPORT {H1–H6} - MP&VRP Performance and Improvement {H2}	2.4	The Contractor shall: (a) provide an electronic weekly 'Performance Assessment Report' to the Authority (MilPers MI Mgr) in the format approved by the Authority in writing prior to the Operational Services Commencement Date and prior to any future changes (for example, any changes to the MP&VRP such as patching/updates or Changes). The 'Performance Assessment Report' shall include, but is not limited to: (i) performance and utilisation metrics of all platform technology layers (including, but not limited to, processor & memory utilisation across all underlying server compute nodes, network bandwidth utilisation, information on database loading, resource consumption, MP&VRP server load in terms of memory and explanations on any dips in performance, particularly week-on-week dips) for the previous week (Monday to Sunday); and (ii) trend analysis across a 13-month rolling average for all metrics; (b) on request of the Authority (MilPers MI Mgr), add, amend and remove data, parameters and metrics to the 'Performance Assessment Report'; (c) provide an electronic monthly 'Assessment Report' to the Authority (MilPers MI Mgr), summarising the performance and efficiency of the MP&VRP as identified in the 'Performance Assessment Report'. The Assessment Report includes but is not limited to technical details, including root cause analysis, for performance issues of MP&VRP raised by the Contractor or the Authority (MilPers MI Team) and changes or technical improvements which	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.7 - 1.3.11

		would improve MP&VRP performance and/or support better MI reporting functionality. (d) deliver, in accordance with the Change Control Procedure, the MP&VRP Changes proposed in the monthly 'Assessment Report' that have been accepted in writing by the Authority (MilPers MI Mgr); and (e) provide the Authority (MilPers MI Team) access to system performance, usage information (including raw data behind reports in this Paragraph 2.4 and ability to create their own analyses) and automated MI information in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1).	
BAU & SUPPORT {H1–H6} - Specialist Technical Advice and Support {H3}	2.5	The Contractor acknowledges that this requirement is to ensure that the Authority (MilPers MI Team) is provided with specialist technical advice and face-to-face support on all areas of the MP&VRP to enable the Authority (MilPers MI Team) to meet their responsibilities in all areas of data management and MI and provide technical support to the Authority's MI Community. Contractor advice and support includes technical and system set up/configuration, 'Data Preservation Repository' (DPR) and any military MI questions. This requirement also includes providing technical support by attending and participating in meetings as required by the Authority (MilPers MI Mgr), including at times, giving technical briefings.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24
BAU & SUPPORT {H1–H6} - Specialist Technical Advice and Support {H3}	2.6	The Contractor shall: (a) upon request from the Authority (MilPers MI Team), provide support to the Authority (MilPers MI Team) within Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1); (b) upon request from the Authority (MilPers MI Team), provide immediate technical advice and/or support, to the satisfaction of the Authority (MilPers MI Team); (c) upon request from the Authority (MilPers MI Team), assess and research technical questions from the Authority (MilPers MI Team) and provide an answer/resolution, to the satisfaction of the Authority (MilPers MI Team); and (d) on at least 24 hours prior written notice from the Authority (MilPers MI Mgr), provide at least one SQEP to attend a meeting where the Contractor's attendance is requested.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24

BAU & SUPPORT {H1–H6} - MP&VRP Service Failure Information {H4}	2.7	The Contractor acknowledges that this requirement is to ensure that Authority (MilPers MI Team) is provided with full and accurate information about incidents in a timely manner by the Contractor, and that this is with sufficient technical detail to enable the Authority (MilPers MI Team and/or the MilPers MI Mgr) to make informed decisions about actions, initiating business continuity arrangements and communicating with the 'Service Management Information Centres' (each of the single services have they own MI team) and/or 'Management Information Centres'.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.1 - 1.3.6
BAU & SUPPORT {H1–H6} - MP&VRP Service Failure Information {H4}	2.8	The Contractor shall: (a) provide the Authority (MilPers MI Team) with technical information (including but not limited to, the reason, impact, solution, estimated resolution time, and proposed customer communications) on all medium or higher impact level MP&VRP failures (in both production and any testing/development environments being used by the Authority) promptly following the initial identification of such failure; (b) for issues not immediately resolvable to the satisfaction of the Authority (MilPers MI Team), provide the Authority (MilPers MI Team) with technical updates on the incident (including, if known, the fix and the expected resolution timescale) every hour during Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1) until a fully functional service is resumed; (c) promptly inform the Authority (MilPers MI Team) of all incidents from impact level 'Medium' upwards that affect the MP&VRP; (d) following the resolution of each MP&VRP failure, provide the Authority (MilPers MI Team) with full details of the resulting investigation, including the reasons for the issue or failure, work undertaken to resolve it, work to prevent future reoccurrence and any ongoing or future potential impact on the delivery of the Services; and (e) when any element of the MP&VRP is not available and/or fully functional during Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1) according to the latest agreed version of the Logical Application Model for the underlying application, provide the Authority (MilPers MI Team) with details of why the element of the MP&VRP is not available and/or fully functional (such	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.1 - 1.3.6

		details to include, but not be limited to, summary of issue, issue owner, action to be, or being, taken, the effect of the issue(s) on platform End Users, expected resolution time and the message to be disseminated to the Authority's 'MI Community'.	
BAU & SUPPORT {H1–H6} - Authority Access to Contractor's Computer System {H5}	2.9	The Contractor acknowledges that: (a) the working practices of the Authority (MilPers MI Team) requires them to have access to the Contractor System for running, downloading, processing, delivering, and filing Management Information Service Request (MISR) reports and associated information (including access to historic Authority MI files and/or miscellaneous documentation held on the Contractor System); and (b) the Authority (MilPers MI Team) may require access outside of Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1) to deal with threat to life, MI requests, or to carry out MP&VRP Field Acceptance Testing.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.25 - 1.3.27
BAU & SUPPORT {H1–H6} - Authority Access to Contractor's Computer System {H5}	2.10	The Contractor shall: (a) provide the Authority (MilPers MI Team) with access to the Contractor System and servers to undertake, with software tooling installed and maintained in line with the MP&VRP, necessary Data Holding reviews, Data analysis, Data Quality validations, and other related Data & MI activities; (b) provide the Authority (MilPers MI Team) with continuous access to the Contractor System (directly to network with Contractor provisioned ICT equipment or alternative connectivity mechanism which provides same functionality and usability); (c) ensure that each team member of the Authority (MilPers MI Team) has a distinct connection available, from an Authority designated location (the availability of which is to be in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1)); (d) ensure vendor provided software tools is made available, installed, and maintained to support and enhance the MP&VRP (including, but not limited to, the following (where software platform changes are made, their equivalent to be made available): 'Structured Query Language' (SQL) Developer, OBIEE Client tools, Informatica & DAC Client tools, ODI Client tools and Microsoft Office tools);	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.25 - 1.3.27

		(e) ensure that each member of the Authority (MilPers MI Team) has continuous access to the underlying systems, servers, databases and services to enable the full functional capability and use of the software tools referred to in this Paragraph 2.10; and (f) ensure that there is capability to seamlessly transfer data to/from the Contractor's network from/to the Authority's network, without restriction excepting necessary security constraints.	
BAU & SUPPORT {H1–H6} - MP&VRP Performance Matrix {H6}	2.11	In order to provide a reporting platform capable of servicing a high concurrent user count, with minimal or nil degradation to service performance, the Contractor shall ensure that the MP&VRP is performant in accordance with the MP&VRP Performance Matrix (as set out in Appendix 1 of Annex H to Schedule 2.1) and in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1).	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.7 - 1.3.11
BAU & SUPPORT - ADDITIONAL {H7–H14} - Provide a MP&VRP Production Support Environment {H7}	3.1	The Contractor acknowledges that during the transformation period of ownership transfer of the MP&VRP reporting capability layer over to Authority ownership and beyond, the Authority (MilPers MI Team) will require access to a production support environment for use to test and prove OBIEE repository data and reporting catalogue changes.	Schedule 4.1 - MIL MI&DATA. Section: 1.7 Taking Command and Control of the data [H34 – H38, H7] Paragraph: 1.7.1 - 1.7.32 Section: 1.8 Provision of access to MP&VRP development, test and product support environments for authorised Authority personnel to undertake design, development and test activities [H7, H37]; Paragraph: 1.8.1 - 1.8.7
BAU & SUPPORT - ADDITIONAL {H7–H14} - Provide a MP&VRP Production Support Environment {H7}	3.2	The Contractor shall: (a) make available to the Authority (MilPers MI Team) an non-obfuscated production support environment for use as a production support capability in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1); (b) ensure that the MP&VRP production support environment incorporate a fully capable reporting layer connected to the live version of the MP&VRP data warehouse (or an equivalent); (c) provide support and maintenance of the production support environment in line with all other environments in the MP&VRP production estate;	Schedule 4.1 - MIL MI&DATA. Section: 1.7 Taking Command and Control of the data [H34 – H38, H7] Paragraph: 1.7.1 - 1.7.32 Section: 1.8 Provision of access to MP&VRP development, test and product support environments for authorised Authority personnel to undertake design, development and

		(d) ensure that the reporting layer (currently OBIEE) is connected to and uses the live version of the MP&VRP data warehouse, or a suitable alternative with a data set of within 24 hours of currency of the MP&VRP production platform; (e) ensure production support environment can support a minimum of 20 simultaneous Authority users, with no loss of performance characteristics in data retrieval or user presentation. (f) ensure a JPA production and associated data sources copy instance is made available as an integrated user interface for this environment; (g) make provision for the addition of other data sources to this production support environment that match the MP&VRP production platform capability in place and/or inclusion of new data sources to meet or evaluate emerging Service Requirements (h) ensure that the Authority (MilPers MI Team) has continuous access to the reporting platform to undertake all reporting layer code and configuration deployments (including, but not be limited to, OBIEE repository database deployments and on-line updates, webcast deployments (or refreshed from production deployments as part of the change process)); and (i) ensure all data security constraints and controls are enabled as per production estate but altered and enhanced as necessary to allow for this capability to be continuously and effectively utilised by the Authority (MilPers MI Team).	test activities [H7, H37]; Paragraph: 1.8.1 - 1.8.7
BAU & SUPPORT - ADDITIONAL {H7–H14} - Maintain MP&VRP to Load, Manage and Store Military HR Information {H9}	3.3	The Contractor acknowledges that this requirement is about the delivery of additional data, system fields and MI supporting items into the MP&VRP as required by the Authority (MilPers MI Mgr).	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.15 - 1.3.21 Section: 1.14 A framework for effective Data Governance
BAU & SUPPORT - ADDITIONAL {H7–H14} - Maintain MP&VRP to Load, Manage and Store Military HR Information {H9}	3.4	The Contractor shall: (a) ensure that any future Business Data fields in JPA or other data source feeding into the MP&VRP are made available in MP&VRP, unless Authority (MilPers MI Mgr) specifically requests their omission, in a format to support MI reporting, and agreed by the Authority (MilPers MI Mgr);	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.15 - 1.3.21

		(b) ensure that alongside the JPA/other source data field(s) that the Contractor creates, configures, and maintains additional fields or items in the MP&VRP to support MI reporting requirements as requested by the Authority (MilPers MI Mgr); and (c) ensure that all data fields in the MP&VRP conform to the Authority (MilPers Data Mgr) definition and syntax rules as notified to the Contractor as part of the Change Control Procedure and, where the definition and syntax rules are not available to the Contractor, it must request them from the Authority (MilPers Data Mgr) in good time to ensure the Authority's Standards are applied).	Section: 1.14 A framework for effective Data Governance
BAU & SUPPORT - ADDITIONAL {H7–H14} - Write-Back Capability in MP&VRP {H10}	3.5	The Contractor acknowledges that this requirement is about providing write-back functionality in the MP&VRP to enable recording of comments against data fields and the creation of new write-back fields.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.12 - 1.3.14
BAU & SUPPORT - ADDITIONAL {H7–H14} - Write-Back Capability in MP&VRP {H10}	3.6	The Contractor shall: (a) ensure that the functionality will not have the ability to change the base HR Data fields held in the MP&VRP or that in JPA/data source; (b) enable capability in MP&VRP for End Users to have a write-back facility on Data fields as defined by Authority (MilPers MI Team); (c) provide Authority (MilPers MI Team) with a housekeeping capability on write-back data to ensure access is available to Authority (MilPers MI Team) to maintain records and enable deletion of write-back data in accordance with HR rules for Business Data set by the Authority (MilPers MI Mgr); (d) provide Authority (MilPers MI Team) with access to change End User's write-back access permissions; (e) record details of all write-back entries made (including, but not limited to, the date/time of the entry and the identity of the author of the entry) and make this information available to the Authority (MilPers MI Team); (f) enable the write-back function on defined selection of data fields to be defined by the Authority (MilPers MI Mgr), or new write-back fields not linked to an existing data field, via the Change Control Procedure; (g) ensure End Users have access to the write-back facility in accordance with Core Hours of Service Availability (as set out in	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.12 - 1.3.14

		Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1); and (h) enable write-back on new data fields as requested by Authority (MilPers MI Mgr).	
BAU & SUPPORT - ADDITIONAL {H7–H14} - Provision of Technical resources to Support MP&VRP {H13}	3.7	The Contractor acknowledges that this requirement is about ensuring that the MP&VRP is supported by competent technical staff that have the knowledge and the experience in the platform's technologies, functionality, and applications.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24
BAU & SUPPORT - ADDITIONAL {H7–H14} - Provision of Technical resources to Support MP&VRP {H13}	3.8	The Contractor shall: (a) provide SQEP to support the MP&VRP in the technologies and functionality of the platform and vendor product set and directly associated technologies (for the support of the MP&VRP reporting delivery capability, the responsibility of supporting this will pass to the Authority on successful delivery of Serial H35, Annex H of Schedule 2.1); (b) provide resources that understand the business usage and data utilised within the Authority's Data Holdings, specifically those used on the MP&VRP; and (c) ensure that all technical resources supporting the MP&VRP are SQEP and have successfully achieved vendor product certification for all applications they use to support the MP&VRP. Certification to be evidenced for all technical resources undertaking support or change activity on the MP&VRP.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24
BAU & SUPPORT - ADDITIONAL {H7–H14} - Management of Access Permissions and Access to MP&VRP {H14}	3.9	The Contractor acknowledges that this requirement is about managing permissions and control access to the MP&VRP and associated data to ensure only authorised individuals can access the functions and data they are authorised to access (this includes the creation of new or changing existing responsibilities and security profiles to support user self-service and/or additional data source(s)).	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.25 - 1.3.27
BAU & SUPPORT - ADDITIONAL {H7–H14} - Management of Access Permissions and Access to MP&VRP {H14}	3.10	The Contractor shall: (a) from the Operational Service Commencement Date: (i) provide access to the Authority (MilPers MI Team) on the MP&VRP for the purpose of changing permissions in MP&VRP in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.25 - 1.3.27

		Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1); (ii) investigate, plan, and amend existing MP&VRP access permissions to conform to permission requirements under any future MP&VRP upgrade, which shall be completed in adherence to the delivery plan (for technical refresh of the platform to ensure Evergreen requirement) and within the technical refresh of the underlying platform; and (iii) administer all account access through the Trusted Route. (b) from the Operational Service Commencement Date until the successful delivery of the requirement in serial H35 of Annex H to Schedule 2.1: (i) create or amended responsibility and/or security profile in next planned change delivery method for MP&VRP, in accordance with the Change Control Procedure, from date of receipt of request from the Authority (MilPers MI Mgr) or within an agreed deadline with the Authority (MilPers MI Mgr); (ii) ensure account access and permissions align with vetting standards and/or DBS Security rules and role-based permissions with access based on a 'Need to Know' requirement; (iii) provide a monthly 'Permissions Extract Report' to the Authority (MilPers MI Team), which shall include, but not limited to, a list of MP&VRP Catalogue items and their access permissions. The 'Permissions Extract Report' shall be in a format which has had the Authority's written approval prior to the Operational Services Commencement Date; and (iv) on receipt of a request from the Authority (MilPers MI Team), deliver an ad-hoc report from the MP&VRP Catalogue Manager to meet the Authority (MilPers MI Team) technical requirements, in electronic format to be approved by the Authority (MilPers MI Mgr).	
DPR REQUESTS {H17–H20} Assessing 'MI Service Requests' (MISRs) {H17}	4.1	The Contractor acknowledges that the historic HR Data for the Armed Forces that existed prior to JPA is held on the DPR system, containing information from over 50 legacy systems and that the Authority routinely receives requests for information held on the DPR, known as 'MI Service Requests' (MISR), which are each assigned a unique MISR number.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.28 - 1.3.32

DPR REQUESTS {H17–H20} Assessing 'MI Service Requests' (MISRs) {H17}	4.2	On receipt of an MISR from the Authority (MilPers MI Team), the Contractor shall promptly: (a) provide written acknowledgement of receipt to the Authority (MilPers MI Team); (b) assess the MISR and make a technical assessment on whether the request can be answered by the DPR (in either a single report output or multiple outputs, the size and nature of such output(s) are dependent on MISR question and its complexity and how the information can be extracted from it); and (c) provide the Authority (MilPers MI Team) with an expert technical assessment on whether the DPR MISR request can be answered by data held on the DPR and how the requirement can be met, including the technical coding of DPR query(s). If DPR Data cannot answer an MISR, the Contractor shall provide the reason(s) why.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.28 - 1.3.32
DPR REQUESTS {H17–H20} Delivering 'MI Service Requests' {H18}	4.3	The Contractor acknowledges that this requirement is about producing and delivering the MISR output as assessed at H17. In delivering the output of the MISR under Paragraph 4.2 (as assessed and approved by the Authority (MilPers MI Team)), the Contractor shall: (a) using an appropriate enquiry tool, extract the MI out of the DPR and deliver the approved technical output to the Authority (MilPers MI Team); and (b) produce and deliver output(s) as a priority service within Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1) when the MISR is for operational or statutory reasons (including but not limited to, Parliamentary Questions, FOI requests and police searches).	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.28 - 1.3.32
DPR REQUESTS {H17–H20} DPR MISR Documentation {H19}	4.4	The Contractor shall provide the Authority (MilPers MI Team) with technical documentation, to the satisfaction of the Authority (MilPers MI Mgr), explaining the development and delivery of the DPR MI output produced under Paragraph 4.3 to meet the Customers' requirements.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.28 - 1.3.32
DPR REQUESTS {H17–H20} DPR Corrections {H20}	4.5	The Contractor shall: (a) ensure the DPR remains accurate, accessible in accordance with security rules, and conforms to any legislative changes to the Data Protection Legislation;	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.28 - 1.3.32

		(b) undertake defined corrections to DPR data, as requested by the Authority (MilPers MI Team), in accordance with the Change Control Procedure; and (c) maintain an audit trail for all changes to DPR and retain such information in accordance with the 'DBS Retention and Disposal Policy'.	
DPR REQUESTS {H17–H20} Training {H22}	4.6	The Contractor acknowledges that this requirement is about delivering specialist and technical training to the Authority's MI community (MP&VRP report writers) including the Authority (MilPers MI Team) on the MP&VRP's functionality, capability, and data sources. For the avoidance of doubt, this requirement does not cover the transfer of knowledge from the Contractor to the Authority as part of the obligation in serial H34 of Annex H to Schedule 2.1 to transfer the MP&VRP reporting delivery capability to Authority ownership. The Contractor acknowledges that, occasionally, the location of the training may be on a MoD site within the UK which is not where the Authority's MilPers MI Team are located.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24
DPR REQUESTS {H17–H20} Training {H22}	4.7	The Contractor shall design, administer, and deliver specialist technical training days on topics and to the frequency as agreed with the Authority (MilPers MI Mgr) (such agreement not to be unreasonably withheld or delayed). Such training shall: (a) include, but not limited to, providing the Authority with training materials (based on examples from the MP&VRP) and accompanying training notes, examples, exercises, and 'How To Guides' as agreed with Authority (MilPers MI Mgr); (b) be delivered on topics including, but not limited to, report development in specific subject areas of MP&VRP (e.g. payroll or future new data sources), using XML, using HTML, and using new MP&VRP MI functionality / analysis packages; (c) reflect the live MP&VRP and content is consistent with MoD standards; (d) be amended or updated as reasonably requested by the Authority (MilPers MI Mgr); (e) require students to complete an Authority (MilPers MI Mgr) approved training feedback questionnaire and the results made available to the Authority (MilPers MI Team). The Contractor agrees that positive feedback shall be considered as the student providing neutral or above markings.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.22 - 1.3.24

MAKE BETTER USE OF INFORMATION AND DATA {H27–H33} Deliver MP&VRP with reporting embedded Data provenance {H32}	5.1	In order for the Contractor to provide MP&VRP End Users information that shows the data lineage from source systems through to the reporting layer, to help minimise incorrect assumptions being made about the Data in the MP&VRP and to allow the End Users to understand the context of the information provided in an MI dashboard/report, the Contractor shall: (a) record the data provenance (including the source of data, business purpose, and any Data transformation undertaken prior to its presentation) for all data presented to the reporting layer in the MP&VRP; (b) ensure that the data provenance is maintained and updated for all new Data items or for modification of existing ones; and (c) make available the data provenance to End Users within the reporting product deployed as part of the Service.	Schedule 4.1 - MIL MI&DATA. Section: 1.3 Provision of Military MI BAU and Support Requirements [H1, H3-H5, H7-H14, H17-H20, H22] Paragraph: 1.3.14 Section: 1.6 Make Better Use of Information and Data [H8 H27 – H33] Paragraph: 1.6.1 - 1.6.12 Section: 1.12 Tracking Data Lineage, Metadata and provisioning Data Provenance [H32, H47] Paragraph: 1.12.1 - 1.12.8
MAKE BETTER USE OF INFORMATION AND DATA {H27–H33} Provide and Maintain MP&VRP Data Warehouse That's Capable Varying Data Refreshing {H33}	5.2	The Contractor shall: (a) provide and maintain a data warehouse for the MP&VRP which allows different Data Holdings to be refreshed (i.e. new/changed data loaded) at different frequencies; (b) in order to provide the capability to have different data refresh capacities and/or frequencies for different data groups in the MP&VRP, establish and maintain 'Full' data loads and 'Incremental' data loads for all data domains sourced into the data warehouse; and (c) agree the capacities and/or frequencies of such data loads with the Authority (Data Domain Owner and MilPers MI Mgr).	Schedule 4.1 - MIL MI&DATA. Section: 1.6 Make Better Use of Information and Data [H8 H27 – H33] Paragraph: 1.6.1 - 1.6.12
DATA COMMAND AND CONTROL {H34–H38} Provide Authority Access to MP&VRP Development and Test Environments {H37}	6.1	The Contractor shall: (a) provide the Authority (MilPers MI Team) with access to non-obfuscated MP&VRP environments to support the Authority (MilPer MI Team) to fulfil its responsibilities on taking ownership of the MP&VRP delivery capability from the Contractor, which includes: (i) ownership of the reporting data model (the reporting model existing in the performant reporting layer - star schema dimensional data model); (ii) ownership, administration and sole material control of the semantic reporting layer (currently OBIEE repository database) that defines the physical data model through to presentation layers of the reporting; and (iii) ownership, administration and sole material control of the reporting catalogue (currently OBIEE webcat) that contains	Schedule 4.1 - MIL MI&DATA. Section: 1.7 Taking Command and Control of the data [H34 – H38, H7] Paragraph: 1.7.1 - 1.7.32 Section: 1.8 Provision of access to MP&VRP development, test and product support environments for authorised Authority personnel to undertake design, development and test activities [H7, H37]; Paragraph: 1.8.1 - 1.8.7

		and controls the user interface collateral (Dashboards and reports); (b) provide and maintain non-obfuscated MP&VRP development and test environment landscape to the Authority (MilPer MI Team) to support change activity for production support and scheduled changes. Environments to include but not limited to: (i) development - for BAU activity; (ii) development - for functional change; and (iii) 'Test for System and Unit Testing'.	
MI AND DATA SHARED REQUIREMENTS {H39–H40}	7.1	The Contractor acknowledges that this requirement is for data knowledge services, including the practice of understanding, documenting and conveying information about data in Data Holdings and Data Flows (where one end of the Data Flow is to/from a Data Holding and the other end of the Data Flow is to/from any other Data Holding, whether or not it is managed by the Contractor under this Agreement)).	
MI AND DATA SHARED REQUIREMENTS {H39–H40} Data Model Schema Documentation Pack {H39}	7.2	The Contractor shall provide and maintain a 'Data Model Schema Documentation Pack' (being a set of documents that technically describe the Data components of ICT system for all Data Holdings and all Data Flows (if applicable)) to the Authority (MilPers MI Team and MilPers Data Team) with the following timescales: (a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing).	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4
MI AND DATA SHARED REQUIREMENTS {H39–H40} Data Model Schema Documentation Pack {H39}	7.3	Each 'Data Model Schema Documentation Pack' shall be produced in an editable electronic format in a medium readily useable by the Authority on a Authority system, as specified by the Authority (MilPers MI Team and MilPers Data Team) and include, but not be limited to, the following: (a) 'Logical Data Model Entity Relationship' diagrams, providing an accurate model of the information requirements of all/part of an organisation which serves as a basis for file and database design but is independent of any specific implementation technique or	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4

		product (with cardinality) in an industry standard modelling tool which is ModNet compliant; (b) 'Physical Data Model Entity Relationship' diagrams, showing how Data has been structured for physical implementation in a database (with cardinality, key relationship columns and granularity constraints) in an industry standard modelling tool which is MoDNet compliant); (c) a 'Data Dictionary' (being a structured description of a database, containing the names and structures of all Data types, and can also hold information such as processing restrictions, Data Quality validation, and rules), with granularity at the table and column level and showing all Data items with datatype definitions, constraints, rules for Business Data (as set by the Authority), the Data Definitions to Business Data and Data transformations, Authority process ownership; and (d) where a Data Flow exists, a Data lineage showing the source and target Data items with any Data transformations for such Data item.	
MI AND DATA SHARED REQUIREMENTS {H39–H40} Reference Data Item Catalogue {H40}	7.4	The Contractor shall provide and maintain a 'Business Reference Data Item Catalogue' (being a document which lists and describes all Reference Data at the Data item level) to the Authority (MilPers MI Team) and Authority (MilPers Data Team): (a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing). (d) each 'Business Reference Data Item Catalogue shall be produced in an editable electronic format in a medium readily useable by the Authority on the Authority System (as specified by the Authority (MilPers MI Team and MilPers Data Team)), be in a structure and with content agreed with the Authority (MilPers MI Team) and including but not limited to the following:	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4

		(i) Reference Data with system and/or system module names; (ii) 'Data group business names' (being the names for a collection of Data items logically related to each other, often for a common business purpose); (iii) Data item business names; (iv) all Data held in an information system or filestore; (v) the 'Data Currency' (being the relevance and applicability of the Data to current business operations, where the Data may be 'current', 'applicable', 'obsolescent', or 'obsolete') of all Data held in an information system or filestore; (vi) the data value description or definition; and (vii) Reference Data structural complexity (for example, simple list of values, any hierarchy details (for example, parent/child hierarchy (where one Data item is logically the owner of another in business terms, so that the owner, the "Parent", may have own one or more instances (or none) of the subordinate Data item, the "Child")) and complexity (for example, embedded in table with code)).	
DATA MANAGEMENT {H41–H48}	8.1	The Contractor acknowledges that this requirement is for the Data management, Data Quality, Data lifecycle, and Data knowledge services relating to the Data contained in Data Holdings and in Data Flows (where one end of the Data Flow is to/from a Data Holding and the other end of the Data Flow is to/from any other Data Holding (whether or not it is managed by the Contractor pursuant to this Agreement)).	
DATA MANAGEMENT {H41–H48} Provision of Data Subject Matter Expertise {H41}	8.2	From the Operational Service Commencement Date, the Contractor shall provide 'Data Subject Matter Expertise' for all Data Holdings and all Data Flows to the Authority (MilPers Data Team) on request. Such 'Data Subject Matter Expertise' shall: (a) consist of all aspects of Data Management, Data Definition and Data Quality of all Data items in all Data Holdings and all Data Flows and delivering or facilitating the delivery of other obligations in Paragraphs 9 and 10 of this Schedule. (b) be delivered by Contractor Personnel who possess the following skills and experience (evidence of which to be provided to the Authority on request): (i) at least a working understanding of the Data Holdings and Data Flows; (ii) experience and knowledge of Data contained in the Data Holdings and Data Flows, and the relevant Software and Hardware processes of that Data; and	Schedule 4.1 - MIL MI&DATA. Section: 1.15 Provision of technical and data SME resource to support the delivery of any relevant wider Data Management requirements and documentation [H41]. Paragraph: 1.15.1 - 1.15.2

		(iii) full knowledge of all relevant aspects of the Contractor's delivery of the Authority's Service Requirements.	
DATA MANAGEMENT {H41–H48} Provision of Data Subject Matter Expertise {H41}	8.3	The Contractor acknowledges that: (a) the frequency of requests Authority (MilPers Data Team) will be between 1 to 12 times per month, with a likely average of 8 times per month; (b) the frequency of regular meetings will be at least once every 3 weeks with a maximum of 1 per week with an estimated normal duration of 30 minutes; (c) the frequency of ad hoc meetings will be between 1 to 12 times per month, with a likely average of 8 times per month and of an estimated duration of 30 minutes, excepting one such meeting with a maximum of 2 hours once per month; and (d) the frequency of face-to-face meetings on the Authority Premises will be at least once every 3 months, with a likely average of 6 times per year and a maximum of 12 times per year, with an estimated average duration of 60 minutes and a maximum of 120 minutes.	Schedule 4.1 - MIL MI&DATA. Section: 1.15 Provision of technical and data SME resource to support the delivery of any relevant wider Data Management requirements and documentation [H41]. Paragraph: 1.15.1 - 1.15.2
DATA MANAGEMENT {H41–H48} Data Quality assurance in design and by recovery {H42}	8.4	From the Operational Service Commencement Date, the Contractor shall provide Data Quality assurance in Data design and by recovery for all Data Holdings and all Data Flows to the Authority (MilPers Data Team). (a) through undertaking Data analysis, Data design, and Data Testing: (i) for each new Data Holding and/or new Data Flow under development at the time of the Operational Service Commencement Date; (ii) for each new Data Holding and/or new Data Flow developed after the Operational Service Commencement Date; and (iii) for each Data Holdings and/or Data Flow subject to the Change Control Procedure; and (b) for new and changed Data items and Data values (including Reference Data values) ensuring that they are fit for purpose in accordance with the Service Requirements (and any associated technical requirements) and Data Quality controls for all Business Data processing and at all points of Data load, Data entry, Data integration, Data interface, update, import and export as required by the Authority and expressed in the Change Control Procedure, including: (i) developing Data processing, screen functions, Data capture functions, Data extract functions, and Data structures to ensure Data Quality is enabled and maintained;	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13

		(ii) providing Automated Update methods that are efficient, accurate, appropriate to the Service Requirement and approved by the Authority, using for example but not limited to system update, enabled Authority or End User screen-based direct entry, or processing data capture inputs such as robotics, forms and files (for example 'Comma Separated Variable' (CSV) or Microsoft Excel formats); and (iii) ensuring that Data Quality unexpected or negative effects or impacts on related Data, dependent Data or affected Data items and values outside of the scope of the Change Control Procedure are brought to the attention of the Authority (MilPers Data Team) to ensure consistent and effective processing and Data Quality continuity.	
DATA MANAGEMENT {H41–H48} Data Quality assurance in design and by recovery {H42}	8.5	The Contractor shall provide Data Quality assurance by recovery to the Authority (MilPers Data Team) for all Data Holdings and all Data Flows from the Operational Service Commencement Date: (a) through recovery, remediation or corrective action through the Change Control Procedure; (b) with corrections to Data items and Data values (including Reference Data values) ensuring that they are fit for purpose in accordance with the Service Requirements (and any associated technical requirements) and Data Quality controls for all Business Data processing and at all points of Data load, Data entry, Data integration, Data interface, update, import and export as required by the Authority and expressed in the Change Control Procedure, including: (i) making corrections to Data values (including Reference Data values) where data fails to be fit for purpose, irrespective of whether the root cause is or is not the result of an omission, incorrect action, failure of process, or failure of quality control by the Contractor; (ii) making changes to Data processing, screen functions, Data capture functions, Data extract functions, and Data structures to ensure data is fit for purpose, irrespective of whether the root cause is or is not the result of an omission, incorrect action, failure of process, or failure of quality control by the Contractor; (iii) making changes to Data Quality controls to ensure data is fit for purpose, irrespective of whether the root cause is or is	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13

		not the result of an omission, incorrect action, failure of process, or failure of quality control by the Contractor; (iv) Monitoring the correction for a period required by the Authority (MilPers Data Team) and reporting where data fails to be fit for purpose (as required in the Data governance and Data Quality reporting capability required in Paragraphs 10.13 and 10.14 of this Part 8 of Schedule 2.1); (v) providing Automated correction methods that are efficient, accurate, appropriate to the Service Requirement and approved by the Authority using, for example but not limited to system update, enabled Authority or End User screen-based direct entry, or processing data capture inputs such as forms and files (for example 'Comma Separated Variable' (CSV) or Microsoft Excel formats); and (vi) Ensuring that Data Quality unexpected or negative effects or impacts of correction on related Data, dependent Data or affected Data items and Values outside of the scope of the correction in the Change Control Procedure are notified to the Authority MilPers Data team to ensure consistent and effective processing and Data Quality continuity.	
DATA MANAGEMENT {H41–H48} Provision of Access to Data Holdings {H43}	8.6	The Contractor shall provide continuous and complete visibility using a real-time access mechanism at the direct data access layer to the production environments of all on-line holdings in Data Holdings for the Authority (MilPers MI Team) and Authority (MilPers Data Team): (a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing).	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4
DATA MANAGEMENT {H41–H48} Provision of Access to Data Holdings {H43}	8.7	The Contractor shall provide real-time access mechanisms to ensure that from the Operational Service Commencement Date all required accesses are provided:	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4

		(a) to Authority nominated staff in accordance with Baseline Security Requirements contained in Annex 1 of Schedule 2.4 (Security Management); (b) to Authority nominated staff using such direct data access layer tools as are appropriate to allow for native data connections to Data Holdings; and (c) in conformance with the Authority's access requirements, the Contractor will provide a user administrative function to activate, maintain and inactivate user accounts, to be provisioned from the Service Desk and to be defined in the Service Catalogue; and access authorisation function to be fully compliant with the extant security requirements, as set out in Schedule 2.4 (Security Management).	
DATA MANAGEMENT {H41–H48} Provision of Access to Data Holdings {H43}	8.8	Within 12 months of the Operational Service Commencement Date, the Contractor shall provide real-time access mechanisms to ensure that all required access is to be available to nominated Authority staff using Authority MODNet devices. Such real-time access mechanisms shall provide suitably authorised Authority staff with an appropriate means of connecting to the Data Holding, using industry standard software tooling specific to the Data Holding container technology: (a) via the connection and software approved by the vendor of the software product supporting the Data Holding for executing 'Structured Query Language' (SQL) where the data is contained in a structured Data Holding (being Data that is held in fixed fields in a Data Holding); (b) via the same product tooling that is used by the Contractor for accessing the data in a Data Holding where the data is contained in a unstructured Data Holding (Data in a format that requires interpretation); (c) using a End User accessed device connectivity available to the Authority staff in their default locations; and (d) with sufficient written and verbal guidance and instruction so that the Authority staff can easily use the mechanisms from the dates of provision described above.	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4
DATA MANAGEMENT {H41–H48} Data Quality Reporting and Tools {H44}	8.9	The Contractor shall provide, maintain, update and issue a Data Governance and Data Quality Reporting capability for all cited Data Holdings and all cited Data Flows to the Authority MilPers Data Team: (a) Providing such capability:	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13

		(i) within 6 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (ii) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (iii) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing); (b) From the Operational Service Commencement Date, the Contractor shall provide a Weekly Data Quality Adherence Report which shall contain: (i) Trend analysis reporting demonstrating the Contractor's adherence to Data Quality, Data integrity and Data security (for example, the function of protecting the Data from inappropriate access, loss and corruption) requirements; (ii) Negative adherence indicators to demonstrate a downward trend across time for those Data items and Data values for which the Contractor has responsibility for quality management to ensure that failings are being remediated; (iii) Quality or integrity failings resulting from any planned or unplanned change activity implemented by the Contractor; (c) From the Operational Service Commencement Date, the Contractor shall provide a Monthly Data Flow Quality Report, which shall contain: (i) The quality of data in all cited Data Flows to or from (including between) Data Holdings; (ii) The rate of data throughput in each Data Flow transaction and of each Data item in a Data Flow; (iii) Details of the data not fit for purpose as defined by approved and documented Authority Requirements and Data Quality controls applied by the Contractor on behalf of the Authority to each Data Flow transaction and to each Data item in the Data Flow to include:	

		(A) The percentage throughput which is not fit for purpose; (B) Details of any Data Quality Characteristic which is not met by the data; (C) Details of any detectable root cause leading to a Data Quality Characteristic not being met; (d) From the Operational Service Commencement Date, the Contractor shall provide a Monthly Data Quality Risk Report which shall contain: (i) Any risk inherent in new Data design or Data change which may cause the data to be not fit for purpose as defined by approved and documented Business Requirements, Technical Requirements and Data Quality controls applied by the Contractor on behalf of the Authority; (ii) Details of the nature of risk, likelihood of risk becoming an issue, timescale in which risk may become an issue, data affected; Personnel Populations affected, volumes per Personnel Population affected, potential impact on the approved and documented Authority Requirements and Data Quality controls, and risks that have disappeared since last reported as a risk; (e) From the Operational Service Commencement Date, the Contractor shall provide a Monthly Data Quality Issue Report which shall contain: (i) any Data Quality issue where the data fails to be fit for purpose as defined by approved and documented Authority Requirements and Data Quality controls applied by the Contractor on behalf of the Authority; (ii) any Data Quality issue detected by the Contractor or reported to the Contractor by others (including users of Data Holdings the Contractor manages, DBS teams, the operators of Data Holdings not managed by the Contractor which interface with Contractor-managed systems, and recipients of exported data or reports); (iii) details of the data at issue, nature of the issue, previously reported risk which has come to fruition as an issue, impact of the issue on approved and documented Authority Requirements and Data Quality controls, consequential effect on related Data and dependent Data, consequential	

		effect on data in other cited Data Holdings and Data Flow (cited or not cited) managed by the Contractor, Personnel Populations affected, volumes per Personnel Population affected, the timescale in which the issue might escalate in impact, and issues that have been fixed since last reported as an issue; (f) From the Operational Service Commencement Date, the Contractor shall provide a Monthly Data Quality Correction Procedure Report which shall contain: (i) issue correction procedures (advocated by the Contractor and agreed by the Authority) for data subjected to Data Quality issues that cannot be eradicated by a fix and which require Authority or user corrective action, where data fails to be fit for purpose as defined by approved and documented Authority Requirements and Data Quality controls that have been applied by the Contractor on behalf of the Authority; (ii) details of the data at issue, the nature of the issue, Personnel Populations affected, volumes per Personnel Population affected, correction procedure agreed with the Authority MilPers Data Team, user of and other participants in the correction procedure, activation process of the procedure, procedural steps that need to be followed; (g) The reports to be provided from the Operational Service Commencement Date shall be: (i) in a structure and with content agreed with and approved in advance by the Authority MilPers Data Team at the Operational Service Commencement Date; (ii) in an editable electronic format in a medium readily useable by the Authority on a MOD system as agreed with the Authority MilPers Data Team at the Operational Service Commencement Date.	
DATA MANAGEMENT {H41–H48} Data Quality Reporting and Tools {H44}	8.10	The Contractor shall provide, maintain, update and issue an industry standard Data Governance and Data Quality Reporting Tool capability for all cited Data Holdings and all cited Data Flows to the Authority MilPers Data Team: (a) Providing such capability: (i) within 6 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date;	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13

		(ii) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (iii) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing); (iv) For the Military Personnel and Veterans MI Reporting Platform within 2 months of completion of a Technical Refresh of the platform after the Operational Service Commencement Date; (b) Providing such capability: (i) in which the Authority shall have access to a data management suite with features to include, but not limited to data profiling, data parsing and data standardisation, identity resolution, data cleansing and enhancement, data auditing and monitoring; (ii) in which the Authority shall have access to industry standard Data Quality reporting tools with the capability described above to allow analysis and investigation of all cited Data Holdings and all cited Data Flows; (iii) which the Contractor shall produce, maintain, and make available to the Authority in accordance with Core Hours of Service Availability (as set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1.	
DATA MANAGEMENT {H41–H48} Provision of Data Information {H45}	8.11	From the Operational Service Commencement Date, the Contractor shall provide and maintain 'Data Information Documents' (being documents setting out information about any aspect of Data managed by the Contractor) to the Authority (MilPers Data Team) in an editable electronic format in a medium readily useable by the Authority on a Authority system, in the structure, and with content as agreed with the Authority (MilPers Data Team) for each request: (a) on request by the Authority (MilPers Data Team), one or more 'Data Information Documents' (as applicable) about any aspect of Data governance, Data management, Data definition, Data lifecycle (including Data design, implementation, Change, Data	Schedule 4.1 - MIL MI&DATA. Section: 1.10 Data Architecture [H39, H40, H43, H45] Paragraph: 1.10.1 - 1.10.4 Section: 1.14 A framework for effective Data Governance

		retention, Data archive and Data disposal), and Data Quality about any Data items in any Data Holding or any Data Flow from a Data Holding. Such 'Data Information Documents' shall fully disclose the values in the Data at any point in end-to-end processing including in any Data Flow (including any flow not listed in the Mil Pers & Vets Primary Data Flow Register) in or out of any Data Holding, and any transaction states and triggers, and in any staging table holding the Data; and (b) where the Authority (Mil Pers Data Team) has requested that a 'Data Information Document' shall be updated on subsequent change automatically update and deliver the document to the Authority (Mil Pers Data Team) when a Data Holding and/or a Data Flow is subject to the Change Control Procedure at the point that Testing starts (or before implementation if there is no Testing).	
DATA MANAGEMENT {H41–H48} 'Data Quality Controls' document {H46}	8.12	The Contractor shall provide, maintain, update and issue a 'Data Quality Controls' document for each Data Holding and each Data Flow to the Authority (MilPers Data Team): (a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing).	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13
DATA MANAGEMENT {H41–H48} 'Data Quality Controls' document {H46}	8.13	From the Operational Service Commencement Date, the Contractor shall provide that each 'Data Quality Controls' document in an editable electronic format in a medium readily useable by the Authority on a Authority system, in the structure, and with content as agreed with the Authority (MilPers Data Team) explains for all Data items: (a) comprehensive details of the Data Quality controls to ensure Data is fit for purpose as defined by Service Requirements (and any associated technical requirements) and Data Quality controls applied for all Business Data processing and at all points of Data entry, Data processing and Data integration; and	Schedule 4.1 - MIL MI&DATA. Section: 1.11 Data Quality Management covering DQ Assurance, Controls and Reporting [H42, H44, H46] Paragraph: 1.11.1 - 1.11.13

		(b) the measures applied to structured Data and unstructured Data to ensure the Data is fit for purpose when the data is captured and when held throughout the life of the data from Data design until Data disposal, which shall include: (i) details of the Service Requirements that provide the reason for the data to be captured, held and processed, including a specification for the data which describes it, its use and the features that make it fit for purpose; (ii) for Reference Data, details of the presentation and use of Values (including but not limited to the menu selection from a list of Controlled Values); (iii) details of the technical requirements that operate on the Data, including but not limited to any 'Mandatory Data' (being Data for which a Value must be present, to meet the business requirement, technical requirement, and data quality controls) status for record creation and processing purposes, and data standards such as date formats, which are presented in recognised standard format to enable data to be fully exploitable and interoperable with other existing and foreseeable systems; (iv) details of End User information services applied, provided or supported, including but not limited to training and education, instruction and guidance, documentation and screen presentation, data source verification, Data Quality validation, generated help and prompts, structure and format, Controlled Values and formulae; (v) details of how Authority-defined Data Quality characteristics (as defined by the Authority and notified to the Contractor) are applied. including but not limited to completeness, validity, accuracy, consistency and timeliness); and (vi) details of any Contractor provision of processes that monitor the quality of the data.	
DATA MANAGEMENT {H41–H48} 'Lineage, Derivation, Transformation and Metadata' document {H47}	8.14	The Contractor shall provide and maintain a 'Lineage, Derivation, Transformation and Metadata' document for each Data Flow and out of each Data Holding (including where the other sending or receiving Data Holding is not managed by the Contractor) to the Authority (MilPers Data Team):	Schedule 4.1 - MIL MI&DATA. Section: 1.12 Tracking Data Lineage, Metadata and provisioning Data Provenance [H32, H47] Paragraph: 1.12.1 - 1.12.8

		(a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing).	
DATA MANAGEMENT {H41–H48} 'Lineage, Derivation, Transformation and Metadata' document {H47}	8.15	The Contractor shall provide that each 'Lineage, Derivation, Transformation and Metadata' document from the Operational Service Commencement Date in an editable electronic format in a medium readily useable by the Authority on a Authority system, in the structure, and with content as agreed with the Authority (MilPers Data Team) which shall: (a) explain for each cited Data Flow the corresponding Data items in Data Holdings at each end of the Flow (where one of the Data Holdings is not managed by the Contractor to include that Data Holding's data provider's reference information); (b) explain metadata details for each Data item including but not limited to the data type (either Reference Data or Dynamic Data), the Reference Data values, any Data mappings, the technical requirements and Service Requirements driving Derivation (being the source(s) of a Data item which from changing the content and/or structure and Data transformation, the 'Mandatory Data' (being Data for which a Value must be present, to meet the business requirement, technical requirement, and data quality controls) and 'Optional Data' (being Data for which a Value may not be present) (and whether 'Mandatory Data' or 'Optional Data' arise from the Service Requirements (and any associated technical requirements) or Data Quality controls), any 'Defaulted Data Values (being a value inserted into the Data structure if no other value is provided for the attribute on creation of a record in the table or file), any indicators and flags, any 'Mapping Rules' (being designed condition applied to the process of transforming Data item value in a sourced Data Holding to be transformed into a meaningful Data item value in a receiving Data Holding) and	Schedule 4.1 - MIL MI&DATA. Section: 1.12 Tracking Data Lineage, Metadata and provisioning Data Provenance [H32, H47] Paragraph: 1.12.1 - 1.12.8

		'Mapping Codes' (being Reference Data value specifically to allow Data item value in a sourced Data Holding to be transformed into a meaningful Data item Value in a receiving Data Holding), and the Data Quality validation and Data Quality controls; (c) explains all Data items at table and column level of granularity; (d) is presented in a structure and with content agreed with and approved in advance by the Authority MilPers Data team at the Operational Service Commencement Date; and (e) is presented in an editable electronic format, in a medium readily useable by the Authority on a Authority system as agreed with the Authority (MilPers Data Team) at the Operational Service Commencement Date.	
DATA MANAGEMENT {H41–H48} Reference Data Change Information Report {H48}	8.16	The Contractor shall provide, maintain, update and issue a 'Reference Data Change Information Report' (being a report to provide information about how Reference Data can be changed) to the Authority (MilPers Data Team) for all cited Data Holdings and all cited Data Flows: (a) within 3 months of the Operational Service Commencement Date, to cover all Data Holdings and all Data Flows at the time of the Operational Service Commencement Date; (b) from Operational Service Commencement Date, to cover all new Data Holdings and new Data Flows (under development at Operational Service Commencement Date and developed since Operational Service Commencement Date) at the point that Testing starts (or before implementation if there is no Testing); and (c) all Data Holdings and all Data Flows subject to the Change Control Procedure after Operational Service Commencement Date at the point that Testing starts (or before implementation if there is no Testing).	Schedule 4.1 - MIL MI&DATA. Section: 1.5 Testing across releases [H24, H25, H48] Paragraph: 1.5.1 - 1.5.2
DATA MANAGEMENT {H41–H48} Reference Data Change Information Report {H48}	8.17	From the Operational Service Commencement Date, the Contractor shall provide that each 'Reference Data Change Information Report' in an editable electronic format in a medium readily useable by the Authority on a Authority system, in the structure, and with content as agreed with the Authority (MilPers Data Team) which shall: (a) explains the technical structure of each Reference Data item (including but not limited to: a simple List of Values; a parent/child hierarchy (where one Data item is logically the owner of another in business terms, so that the owner, the “Parent”, may have own one or more instances (or none) of the subordinate Data item, the “Child”); embedded in a table structure with supporting code); and	Schedule 4.1 - MIL MI&DATA. Section: 1.5 Testing across releases [H24, H25, H48] Paragraph: 1.5.1 - 1.5.2

		explains the time, resource and technical complexity of change to make an addition, an amendment and a deletion to the Reference Data values, to sufficiently understand the amount of time taken typically to make such changes, the levels and resource skills required typically for such changes, and the degree of technical complexity).	
Schedule 2.1, Part 13 (IT Service Management)			
M1 IT Service Management - Adopting The ITIL Framework and its Extended Use To Support Business Services	1.1	Implement and maintain a Mature IT Service Management (ITSM) capability across all Services and for all ITIL processes and functions, ensuring a measurable progression Maturity of its ITSM capability, using an Authority agreed best practice framework as set out in the Service Operations Manual.	Schedule 4.1 - Common Technical and Enabling Services Section: 8 Software and Licensing Section: 12 Service Management and ITSM Section: 1.1 Application Support Management (AMS)
	1.2	Conduct ITSM Maturity Assessments to ensure continual Maturity of the ITSM capability and confirm the Maturity Level on the Operational Services Commencement Date + 2 months and on each anniversary of the Contract Year thereafter until the final Contract Year when the final assessment must be undertaken 2 months prior to end of the Term.	
	1.3	Schedule and provide SQEP attendees at a monthly review meeting within 3 Working Days following the end of each relevant month.	
	1.4	From Operational Services Commencement Date, arrange and provide a monthly review meeting for SQEP attendees with the Authority (Tech Assurance). Such meeting to be fully minuted and will review outputs and adherence to metrics for the ITSM process area. Improvement activities to be recorded and actioned within mutually agreed timescales.	
M2 IT Service Management - Adopting The ITIL Framework and its Extended Use To Support Business Services	2.1	Submit to the Authority a draft Service Operations Manual in accordance with the timescales detailed in Paragraph 3 (The Service Operations Manual (SOM)) of Part 13 (IT Service Management) of Schedule 2.1.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.5 ITSM Maturity Assessment [M1, M2] Section: 12.6 ITSM Transition Stage [M1, M2, M3] Section: 12.33 Service Catalogue [M1, M2, M4]
	2.2	Maintain the Service Operations Manual and submit to the Authority a revised Service Operations Manual as required in Paragraph 3.7 (Updates to and maintenance of the Service Operations Manual) of Part 13 (IT Service Management) of Schedule 2.1.	

M3 IT Service Management - Adopting The ITIL Framework and its Extended Use To Support Business Services	3.1	Meet and adhere with the service metric targets and Measures of Performance that are contained within the Service Operations Manual.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.6 ITSM Transition Stage [M1, M2, M3] Section: 12.34 Service Level & Service Level Management [M1, M3, M30] Section: 12.51 Service Reporting [M1, M3, M18, M30] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.4 - 16.6.7, 16.6.12
	3.2	Provide the Authority with a report on the services metrics within 5 Working Days of the beginning of each Service Period which will show all metrics and their adherence status, with a commentary of non-adherence and corrective action being applied.	
M4 IT Service Management - Adopting The ITIL Framework and its Extended Use To Support Business Services	4.1	Create, maintain and provide a Service Catalogue with the following timescales: (a) 40 days following the Operational Services Commencement Date, provide the Service Catalogue to the Authority (Tech Assurance, Change Mgr) for approval; and (b) 3 months after Operational Services Commencement Date and whenever updates occur thereafter, provide an updated Service Catalogue to the Authority (Tech Assurance) for approval.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.33 Service Catalogue [M1, M2, M4]
M5 Service Disaggregation and SIAM	5.1	Reach full Disaggregation for all Services operating through a Pseudo SIAM capability within 4 years from Operational Services Commencement Date.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.2 ITSM Transformation Approach [M1, M5,M6, M10, M30] Section: 12.3 ITSM Transformation Plan [M1, M5, M6, M10] Section: 12.4 ITSM Work packages [M1, M5, M6, M10] Section: 12.12 ITSM Transformation (Evolve to Pseudo SIAM) [M1, M5, M6, M29, M30] Section: 12.13 Full Disaggregation and Pseudo-SIAM [M1, M5, M6] Section: 12.14 ITSM Transformation Mode (Available for Full SIAM) [M1,

			M5, M6, M27] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.17 ITSM Tooling as a Tower Service [M1, M5, M6, M30, M31, M37] Section: 12.65 ITSM Governance and Operational Meetings [M1, M5, M6] Section: 12.66 SIAM Introduction [M1, M5, M6, M10, M14, M30] Section: 12.67 SIAM ITIL-aligned Processes [M1, M5, M6, M13, M14, M25] Section: 12.68 SIAM Organisations [M1, M5, M6, M14, M29, M30] Section: 12.69 SIAM Operational Service [M5, M6, M29, M30] Section: 12.70 SIAM Delivery [M1, M5, M6, M14, M26] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.73 SIAM Service Components [M1, M5, M6, M14, M25] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.76 SIAM Service Transition [M1, M5, M6, M14, M37] Section: 12.77 SIAM Service Design [M1, M5, M6, M34]

			Section: 12.78 SIAM Continual Service Improvement [M1, M5, M6, M14] Section: 12.79 SIAM Service-Wide Processes and Functions Section: 12.80 SIAM Maturity Assessment [M1, M5, M6, M14, M26]
M6 Service Disaggregation and SIAM	6.1	Ensure the seamless transition to a Service Integration and Management (SIAM) and Tower Service operating model for all the Services.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.2 ITSM Transformation Approach [M1, M5,M6, M10, M30] Section: 12.3 ITSM Transformation Plan [M1, M5, M6, M10] Section: 12.4 ITSM Work packages [M1, M5, M6, M10] Section: 12.12 ITSM Transformation (Evolve to Pseudo SIAM) [M1, M5, M6, M29, M30] Section: 12.13 Full Disaggregation and Pseudo-SIAM [M1, M5, M6] Section: 12.14 ITSM Transformation Mode (Available for Full SIAM) [M1, M5, M6, M27] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.17 ITSM Tooling as a Tower Service [M1, M5, M6, M30, M31, M37] Section: 12.18 The Contractor's Alignment/Compliance Policies, Regulations & Standards [M8] Section: 12.19 Cabinet Office Technology Code of Practice [M8] Section: 12.20 Government Digital Service (GDS) Standards [M8] Section: 12.65 ITSM Governance and Operational Meetings [M1, M5,

			M6] Section: 12.66 SIAM Introduction [M1, M5, M6, M10, M14, M30] Section: 12.67 SIAM ITIL-aligned Processes [M1, M5, M6, M13, M14, M25] Section: 12.68 SIAM Organisations [M1, M5, M6, M14, M29, M30] Section: 12.69 SIAM Operational Service [M5, M6, M29, M30] Section: 12.70 SIAM Delivery [M1, M5, M6, M14, M26] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.73 SIAM Service Components [M1, M5, M6, M14, M25] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.76 SIAM Service Transition [M1, M5, M6, M14, M37] Section: 12.77 SIAM Service Design [M1, M5, M6, M34] Section: 12.78 SIAM Continual Service Improvement [M1, M5, M6, M14] Section: 12.79 SIAM Service-Wide Processes and Functions Section: 12.80 SIAM Maturity Assessment [M1, M5, M6, M14, M26]

	6.2	Provide the Transformation Plan in accordance with Schedule 6.1 (Transition and Transformation Plan) for the development and implementation of a SIAM and Tower Service Operating model (taking input from the independent assessment) for Authority (Hd Mil Pers & Vets Change) approval which shall: (a) provide a clear plan for developing and evolving the maturity and readiness of all ITSM processes over the course of the contract term in readiness for the transition to a mature SIAM and Tower Service Operating model at expiry of the Term; and (b) be incorporated into the ITSM Maturity Assessments and be subject to all associated requirements.	
	6.3	Following approval, implement the Transformation Plan to achieve the following milestones: (a) 4 years after Operational Services Commencement Date, establish an effective SIAM and Tower Service operating model capability with full Disaggregation of all the Services in accordance with the agreed plan; (b) 5 years after Operational Services Commencement Date, establish SIAM and Tower Service operating model readiness; and (c) 7 years after Operational Services Commencement Date, be able to transition seamlessly to a full SIAM and Tower Service operating model.	
M7 Architecture Management	7.1	From Operational Services Commencement Date and every month thereafter, provide to the Authority (Tech Assurance) within 3 Working Days of the end of the previous month, a detailed report (and further agreed outputs) on the AMO delivery, with agreed performance criteria and adherence to the metrics in the Service Operations Manual.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.9 Architecture and Operations Governance. [M7, M8, M27, M28, M30]
	7.2	From Operational Services Commencement Date and every month thereafter, schedule and provide SQEP attendees at a monthly review meeting of AMO delivery with the Authority (Tech Assurance) within 6 Working Days of the previous month. Meeting to be fully minuted and will review outputs and adherence to metrics for Joint Architecture Board. Improvement activities to be recorded and actioned within mutually agreed timescales	
	7.3	From the Operational Services Commencement Date, provide to the Authority (Tech Assurance) a Sustainability Plan which the Contractor is to be review and update Quarterly, in line with changes to the ICT used to deliver the services, in support of the Agreement and changes to	

		legislation. It must also include recommendations based on ICT developments and industry best practice that would deliver environmental improvements.	
	7.4	From the Operational Services Commencement Date, create Roadmaps for each of the Technology areas used to deliver the Services, help facilitate informed planning and decisions around changes and provide more than just vendor support dates and must consider business and data changes (described in the equivalent roadmaps). The review the Roadmap and sustainability plans with the Authority (Tech Assurance) at least every 3 months.	
	7.5	Commencing 3 months following the Operational Services Commencement Date, adhere to the defined service metric targets to be achieved for AMO delivery at all times, unless agreed otherwise with the Authority (Tech Assurance).	
	7.6	Produce, maintain and make accessible to the Authority (Tech Assurance) at all times, AMO and JAB artefacts, including (but not limited to) models, roadmaps, standards, policies. Changes to artefacts should be made available to the Authority (Tech Assurance) within 2 Working Days of completion.	
	7.7	6 months following the Operational Services Commencement Date, develop and provide a reference model for each 'Architecture Domain', 'Business', Data and 'Application/Technology'. These should provide a logical framework describing each of these areas. For each domain, Roles and responsibilities must be defined and a RACI matrix provided. A tool should then be adopted utilising the reference models and various views of the Enterprise provided as required.	
M8 Architecture Management	8.1	Provide ICT applications, tools, systems and Services which adhere to the DBS Mil Pers & Vets Design Standards and Principles in all areas of the Services.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.9 Architecture and Operations Governance. [M7, M8, M27, M28, M30] Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37]

			Section: 12.18 The Contractor's Alignment/Compliance Policies, Regulations & Standards [M8] Section: 12.19 Cabinet Office Technology Code of Practice [M8] Section: 12.2 Government Digital Service (GDS) Standards [M8]
	8.2	Where the DBS Mil Pers & Vets Design Standards and Principles cannot be adhered to, this to be formally notified with detailed justification to the Authority (Tech Assurance) for agreement to waive.	
	8.3	At least once a month following Operational Services Commencement Date, provide DBS Mil Pers & Vets Design Standards and Principles document updates to the Authority (Tech Assurance) for consideration.	
M9 Architecture Management	9.1	Provide access to Contractor hosted services & tooling for Authority staff using MOD provisioned End User accessed devices on MOD network, in accordance with: (a) Contractor-provided tools, services and resources, defined within this Agreement, are to be made available and accessible by Authority or Embedded Contractor staff at the individual's regular place of work and utilising their MOD provisioned EUD on MOD network, in line with any and all specific requirements detailed with this agreement; and (b) to be provided with appropriately approved and aligned security provisions, to ensure Authority to Operate such service.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37]
	9.2	From Operational Services Commencement Date until enablement of this capability (at 6 months following the Operational Services Commencement Date), with agreement of the Authority (Tech Assurance), enable access via Contractor provided devices.	
M10 Application Transformation	10.1	Ensure that the Service Desk software tooling, used to provide the single Service Desk capability, is capable of being integrated with the MOD ISS standard Operational Service Management (OSM) Service Desk capability, to allow for ticket exchange of summary details and ticket status.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.2 ITSM Transformation Approach [M1, M5,M6, M10, M30] Section: 12.3 ITSM Transformation Plan [M1, M5, M6, M10] Section: 12.4 ITSM Work packages [M1, M5, M6, M10] Section: 12.15 ITSM Tooling Transition to Existing Service [M1,

			M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.66 SIAM Introduction [M1, M5, M6, M10, M14, M30]
	10.2	Within 6 months following the Operational Services Commencement Date, provide a detailed Implementation Plan for Authority (Head Mil Pers & Vets Change, Tech Assurance) approval for enabling the requested integration, including (but not be limited to) describing the requirements, solution, benefits, dependencies, scope, risks, costs, timescales and outputs.	
M11 Application Transformation	11.1	Contribute to the DBS Continuous Improvement strategy by analysing and proposing opportunities for exploitation of developments in technology and services offered by both existing and new third party vendors in order to realise benefit for DBS, it's customers, and improve the experience of the End Users:	Schedule 4.1 - Common Technical and Enabling Services Section: 12.62 Continual Service Improvement [M1, M11] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37]
	11.2	Propose areas where JPA End User capability can be pro-actively improved to introduce; Improved transaction times, beneficial functional enhancements, End User experience benefits;	
	11.3	Within 1 year following the Operational Services Commencement Date and each Quarter thereafter (unless agreed with the Authority (Tech Assurance)), provide the Authority with a report to the Authority (Tech Assurance) aligned to the DBS Continuous Improvement strategy, using the ITSM Continual Service Improvement Procedures detailing opportunities, options, benefits, risks and recommendations for exploiting developments in technology and services. Opportunities that are identified for exploitation will continue to be reported on over time until they either become viable or irrelevant;	
M12 Application Transformation	12.1	At Operational Services Commencement Date, provide a detailed implementation plan for Authority (Head Mil Pers & Vets Change, Tech Assurance) approval for enabling the requested enhanced access which shall include (but not be limited to):	Schedule 4.1 - Common Technical and Enabling Services Section: 9 Service Management and

		(a) the plan, design, and implemented solution must adhere in full with the Security and Information Asset requirements as set out in Schedule 2.4 (Security Management); (b) a description of the requirements, solution, benefits, dependencies, scope, risks, costs, timescales and outputs; and (c) a forecast of take-up of usage across each functional area and may propose a phased implementation based on that profiling.	ITSM Paragraph: 9.11
	12.2	Within 18 months of the Operational Services Commencement Date in accordance with the approved plan, provide enhanced access for End Users to securely access JPA functionality, using MOD or non-MOD managed devices, including access via the internet. JPA functionality to be available via the new enhanced access to include, but not be limited to; (a) Absence; (b) expenses; (c) journey authorisation; (d) pay; (e) personal data functions; and (f) appraisal.	
M13 Application Transformation	13.1	At Operational Services Commencement Date, provide an implementation plan for Identity and Access Management (IdAM) integration across all services Authority (Head Mil Pers & Vets Change, Tech Assurance) approval, to include but not be limited to; describing the requirements, solution, benefits, dependencies, scope, risks, costs, timescales and outputs. Which shall include: (a) a phased roll-out across services and applications, to align with the Technical Refresh and Transformation of the underlying platforms; (b) plan, design and implemented solution capability must adhere in full, with the Security and Information Asset requirements as defined in Annex C; and (c) ICT enabled projects requiring Identity and/or Access Management services shall include the MOD Ent-IdAM service in their assumptions and dependencies. The Contractor will engage, via the Authority (Tech Assurance), with ISS, to explore the possible use of Ent-IdAM.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.67 SIAM ITIL-aligned Processes [M1, M5, M6, M13, M14, M25] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36]
	13.2	Commencing 2 years following the Operational Services Commencement Date and completing 4 years following the Operational Services Commencement Date, update the Services in accordance with the	

		approved plan to be able to support, integrate with, and inform / interface with, a single IdAM solution.	
M14 Application Transformation	14.1	In conjunction with the JPA Technical Refresh activities, provide a data integration platform implementation plan for Authority (Tech Assurance and AH Mil Ops) approval. The plan is to include but not be limited to; describing the requirements, solution, benefits, dependencies, scope, risks, benefits, costs, timescales, outputs, phased integration deployment for all interfaces. The plan must address the following (but not be limited to): (a) Deprecation and removal of the existing point to point integrations to be actively undertaken; and (b) Demonstrate via planning, a logical and phased introduction of new platform and the removal of existing.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.53 Data Management Scheduling [M1, M14] Section: 12.66 SIAM Introduction [M1, M5, M6, M10, M14, M30] Section: 12.67 SIAM ITIL-aligned Processes [M1, M5, M6, M13, M14, M25] Section: 12.68 SIAM Organisations [M1, M5, M6, M14, M29, M30] Section: 12.70 SIAM Delivery [M1, M5, M6, M14, M26] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.73 SIAM Service Components [M1, M5, M6, M14, M25] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.76 SIAM Service Transition [M1, M5, M6, M14, M37] Section: 12.79 SIAM Service-Wide Processes and Functions Section: 12.80 SIAM Maturity Assessment [M1, M5, M6, M14, M26]
	14.2	6 months following implementation of the platform, provide a Benefit Realisation assessment paper to the Authority (Tech Assurance).	

	14.3	4 years following the Operational Services Commencement Date, provide and maintain a flexible, modular and robust data integration platform capability for the Services in accordance with the phased plan (as agreed with the Authority) allowing the Authority to efficiently introduce interactions and interfaces across existing or new data domains and systems. The platform must accommodate the constraints and expectations as established in the Mil Pers & Vets Design Standards and Principles. These to be evidenced in the design and operational capability of the delivered service. In addition to an adherence to the Mil Pers & Vets Design Standards and Principles, the data integration platform shall have the following characteristics: (a) to be designed around a common Mil Pers & Vets Business Glossary/Data Dictionary (see Annex H (Mil MIT & Data)); (b) Data movements inter and intra the Data holdings must be provided as flexible service oriented offerings; (c) the Authority Data shall remain a single and authoritative version of the true people picture; (d) full audit trail of data movements to be maintained and available to the Authority; and (e) providing a flexible and easily adapted integration service methodology which allows for MOD business systems to subscribe to data services within the Mil Pers & Vets data domains;	
M15 Application Transformation	15.1	Deliver the Authority Evergreen and Vendor Support requirements (as established in Part 15 of Schedule 2.1 (Technology)).	Schedule 4.1 - Common Technical and Enabling Services Section: 11 Evergreening Section: 12.22 Service Strategy [M1, M15]
	15.2	Provide a detailed Technology Roadmap to the Authority (Tech Assurance) for approval at the Operational Services Commencement Date and Quarterly thereafter encompassing the period of the Term and 2 years beyond, to show the complete set of technical refresh activities of all hardware and software components that make up the Service.	
	15.3	12 months prior to expiry of Agreement, agree with the Authority (Tech Assurance & Commercial) that the Evergreen requirements of n-1 compliance, non-obsolescence and 2 years support after the Contract Expiry or Termination Date for all hardware and software will be met.	

M16 Application Transformation	16.1	Remove web browser compatibility dependency from all Authority Applications on End User access devices within 2 years following the Operational Services Commencement Date by doing the following: (a) ensure all Services are 'Browser Agnostic' on all End User access devices; (b) ensure Authority's Application usage to not be dependent on a specific client browser vendor & version on the MOD End User access device; and (c) ensure the Authority's access to Applications is not a constraint to adopting the latest MOD End User access device roll-out.	Schedule 4.1 - Common Application and Support Services Section: 5.3 Transforming the Authority's self-service customer function Schedule 4.1 - Overall Approach to Transformation Section: 3 Approach to removing browser dependencies
M17 Application Transformation	17.1	Ensure ICT used to deliver the Services in support of this Agreement are compatible with all End User devices.	Schedule 4.1 - Common Application and Support Services Section: 5.3 Transforming the Authority's self-service customer function Schedule 4.1 - Overall Approach to Transformation Section: 3 Approach to removing browser dependencies
	17.2	Perform development and testing in line with the extant MOD ISS-issued 'Application Developers Guide(s)' (or equivalent) at the time and associated advisory documentation, noting any planned/proposed hardware/software upgrades to ensure compatibility and accessibility from the primary Information Systems provided by MOD ISS to the following End User communities: (a) MOD UK fixed; (b) MOD UK overseas; (c) MOD land deployed; and (d) MOD maritime deployed.	
	17.3	In alignment with Schedule 8.2 (Change), all test materials, including (but not be limited to) test plans, test completion reports and test scripts) must evidence the adherence to this requirement.	
	17.4	Each January following the Operational Services Commencement Date, provide to the Authority (Tech Assurance) an annual assessment of testing requirements for DBS MPV applications when mapped against the technology roadmaps for the primary four End User communities identified above. The report is to include but not be limited to: (a) emerging risks; and	

		(b) proposed changes to testing strategy.	
M18 Application Transformation	18.1	At all times following Operational Services Commencement Date, provide the Services in accordance with the Non-Functional Requirements (as detailed in Appendix 1 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.51 Service Reporting [M1, M3, M18, M30]
	18.2	within 5 Working Days of the end of each month, produce a monthly report detailing NFR compliance (and non-compliance) for the preceding month to the Authority (Tech Assurance).	
M19 Exploit Existing Investments	19.1	At Operational Services Commencement Date, produce a 'Customisation Assessment Report' for Authority (Tech Assurance) approval which shall apply to all COTS products where CEMLI's or their equivalent have been deployed, and not limited to the JPA application, including (but not be limited to): (a) identifying customisations and record the detailed justification for their usage over standard functionality; (b) establishing and documenting in detail, any opportunities for standardisation and enhanced use of native/standard functionality; (c) providing a measurable set of deliverables, whereby the required changes will be incorporated into planned projects where possible and enforced though well-defined standards; and (d) identifying where subsequent releases of the underlying product can provide native capability to remove or reduce the customisation in place.	Schedule 4.1 - Common Technical and Enabling Services Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.4
	19.2	Update and provide to the Authority (Tech Assurance) for approval the 'Customisation Assessment Report', under the following conditions: (a) within 30 Working Days of Transition Services activity altering the baseline of the customisations in use; and (b) within 60 Working Days of a new release of the COTS product being announced by the third party vendor, which provides native capability to reduce or remove customisations.	
	19.3	Undertake an ongoing review of all system designs and configuration artefacts to record their purpose, usage and relationship to the business requirements and processes to thereby propose a means to reduce the number and complexity of bespoke components.	
M20 Exploit Existing Investments	20.1	At Operational Services Commencement Date, provide a comprehensive report on capacity management usage and compliance across the Authority System to the Authority (Tech Assurance) for approval, to include but not be limited to:	Schedule 4.1 - Common Technical and Enabling Services Section: 8 Software and Licensing Section: 12.23 Demand

		(a) development; (b) testing; (c) training; (d) production; and (e) DR.	Management [M1, M20] Section: 12.31 Capacity Management [M1, M20] Section: 12.42 Software Asset and Licence Management [M1, M20]
	20.2	Immediately notify the Authority (Tech Assurance) of any Software license compliance issues identified within the Authority System or associated with the use of Services provided to the Authority, within 5 Working Days of the same being identified by the Contractor.	
	20.3	Provide updates to the report biannually or where licence usage changes and provide an updated report to the Authority (Tech Assurance) within 5 Working Days of the change design being approved. (a) At Operational Services Commencement Date and then on a biannual basis, provide a report for Authority (Tech Assurance) approval, identifying savings opportunities available by consolidating or rationalising product use, environment scope or providing solution alternatives.	
M21 Exploit Existing Investments	21.1	Hold under consideration the use of DaaP(H) platform capabilities prior to any other considerations.	Schedule 4.1 - Common Application and Support Services Schedule 4.1 - Overall Approach to Transformation Section: 2 Application Transformation Paragraph: 2.7
	21.2	Ensure that all Change and Technical Refresh documentation, where related to platform hosting, must support the need for the Contractor to liaise with Authority (Tech Assurance) and ISS to ensure that DaaP(H) service/hosting options are considered in any change.	
M22 Exploit Existing Investments	22.1	Ensure their ability to administer and support the Contractor Technical Infrastructure and deliver the Services as set out in this Agreement, is not impacted by any Service Downtime to the Authority or third party Network Infrastructure.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.28 IT BC, DR & IC Management [M1, M22] Section: 12.29 Service Continuity & Disaster Recovery – Test Assurance Levels [M1, M22] Section: 12.30 Availability Management [M1, M22, M30, M31] Paragraph: 12.30.6

			Section: 12.54 IT Operations Management [M1, M22, M34,M35,M36]
	22.2	Loss of connectivity to the MCN from Contractor Premises must not prevent Contractor Personnel from undertaking their technical or business activity in support of this Agreement.	
	22.3	Provide to the Authority (Tech Assurance) a monthly report detailing network availability for all networks the Contractor is dependent upon in the delivery of the services.	
M23 Exploit Existing Investments	23.1	Undertake decommissioning of any equipment, hardware, software and facility/building in accordance with MOD policy or guidelines and within the Change Management Guidelines.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.56 Infrastructure and Software Management [M1, M23, M38] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	23.2	Inform the Authority (Tech Assurance) in writing, within 5 working days of the intention being known, to decommission any part of the IT estate including buildings and facilities, regardless of the method of disposal.	
M24 Standardisation	24.1	Provide, maintain and manage a Hardware and Software patching strategy, in accordance with the patching requirements and timescales (as detailed in Appendix 3 to this Annex) in full alignment with the Change Management Procedures.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.59 Patching Services [M1, M24, M33, M38] Section: 12.60 Backup Services [M1, M24] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.10 - 16.6.11
	24.2	Provide measures within the Change Management Procedures and the Service Operations Manual.	
	24.3	Provide Patch history documentation within 1 Working Day of the Patch being applied to the Authority (Tech Assurance, SO1 Sy) on request.	
M25 Standardisation	25.1	Provide, maintain and manage Anti-Virus Software updates, in accordance with the patching requirements and timescales (as detailed in Appendix 3 to this Annex) in full alignment with the Change Management Procedures and the Service Operations Manual.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.58 Anti-Virus (AV) Services [M1, M25, M38] Section: 12.67 SIAM ITIL-aligned

			Processes [M1, M5, M6, M13, M14, M25] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.73 SIAM Service Components [M1, M5, M6, M14, M25] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.9
	25.2	Provide AVS history documentation within 1 Working Day of the Update being applied to the Authority (Tech Assurance, SO1 Sy) on request.	
M26 Increased Portability	26.1	At Operational Services Commencement Date, agree a plan with the Authority (Head Mil Pers & Vets Change, Tech Assurance) for how all existing applications and technology within the IT Infrastructure will be migrated to Cloud (or Cloud-hybrid) services with IaaS as the minimum level unless agreed by the Authority (Head Mil Pers & Vets Change, Tech Assurance).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.70 SIAM Delivery [M1, M5, M6, M14, M26] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.80 SIAM Maturity Assessment [M1, M5, M6, M14, M26] Section: 12.87 Increased Portability and Shift to Cloud [M26]
	26.2	Within 4 years of the Operational Services Commencement Date, complete the migration of all existing services within the Authority ICT infrastructure to Cloud services as agreed in the plan, unless agreed	

		otherwise with the Authority (Head Mil Pers & Vets Change, Tech Assurance).	
M27 Supporting the Authority Role	27.1	Support the Authority (Tech Assurance) in its Enterprise Architecture strategy generation and implementation by: (a) making reasonable regular and proactive contributions (recommendations, advisements, industry knowledge and briefings) to the creation of Service Strategy and comply with Authority strategy generation and implementation processes as they evolve; (b) supporting the Authority (Tech Assurance) on request in the activities required to perform assessments on the current state of Services in delivering to the Authority's strategic objectives for Services; and (c) supporting the Authority in Demand Management and the development of new or improved Services.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.7 Architecture and Operations Governance. [M7, M8, M27, M28, M30] Section: 12.9 Architecture and Operations Governance. [M7, M8, M27, M28, M30] Section: 12.14 ITSM Transformation Mode (Available for Full SIAM) [M1, M5, M6, M27] Section: 12.38 Knowledge Management [M1, M27, M28, M30] Section: 12.86 Supporting the Authority Role [M27]
	27.2	From Transition Commencement Date and in accordance with the Enterprise Architecture requirements of this Agreement, provide information, advice and access to SQEP technical and domain resources to the Authority (Tech Assurance) to meet their strategic objectives.	
M28 Supporting the Authority Role	28.1	From Operational Services Commencement Date onwards: (a) provide direct access for all Authority staff (Tech Assurance) to all third party Software and Hardware vendor support services and capabilities across all applications and technology stack that are used to deliver the Services, with the ability for the Authority to view service requests, problem records, and knowledge materials pertinent to the Services; and (a) where direct access to third party vendor support services are not available to the Authority, provide a report to the Authority (Tech Assurance) of any service request or problem record pertinent to the Service provision within 1 Working Day of the request being raised.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.9 Architecture and Operations Governance. [M7, M8, M27, M28, M30] Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.38 Knowledge Management [M1, M27, M28, M30]
M29 Supporting the Authority Role	29.1	Ensure that resource capabilities match the requirements of the roles across all levels of the Contractor organisation: (a) all Contractor resources in team leadership, senior management or influencing roles relating to the provision of IT Services must have experience of working in environments which match the Authority's desired end state (namely with practical ITSM and/or SIAM);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.11 ITSM Existing Model [M1, M29, M30] Section: 12.12 ITSM Transformation (Evolve to Pseudo SIAM) [M1, M5,

		(b) Contractor senior manager resources must have experience of transitioning similar scales of organisation from the current to the target mode of operation; and (c) evidence to be provided prior to instantiation of person in role. This must be evidenced with an experience statement and / or CV for these individuals, which the Authority will need to approve prior to taking up positions within the account;	M6, M29, M30] Section: 12.68 SIAM Organisations [M1, M5, M6, M14, M29, M30] Section: 12.69 SIAM Operational Service [M5, M6, M29, M30] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37]
	29.2	10 Working Days prior to an acceptance interview being conducted by the Authority, make available to the Authority (Tech Assurance) the resume, CV and/or experience statement of candidates being proposed.	
M30 Supporting the Authority Role	30.1	Provide the Authority with real-time, read only access to service information relating to the Services for up to 10 Authority (Tech Assurance) nominated staff, including (but not limited to): (a) all System and Service Management tooling and metrics, including monitoring, alerting, performance, capacity management tools (service metrics required in a dynamic dashboard view; the Authority expects to have flexibility in determining which metrics need to be reported on); (b) asset, inventory and Configuration Management Database (CMDB); (c) Incident and Problem management system; and (d) all test plans, test scripts and test results, through the chosen test tool(s).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.2 ITSM Transformation Approach [M1, M5,M6, M10, M30] Section: 12.9 Architecture and Operations Governance. [M7, M8, M27, M28, M30] Section: 12.11 ITSM Existing Model [M1, M29, M30] Section: 12.12 ITSM Transformation (Evolve to Pseudo SIAM) [M1, M5, M6, M29, M30] Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.17 ITSM Tooling as a Tower Service [M1, M5, M6, M30, M31, M37] Section: 12.30 Availability Management [M1, M22, M30, M31] Section: 12.34 Service Level & Service Level Management [M1, M3, M30] Section: 12.35 Security

			Management [M30] Section: 12.37 Change and Evaluation Management [M1, M30] Section: 12.38 Knowledge Management [M1, M27, M28, M30] Section: 12.41 Asset Management [M1, M30] Section: 12.51 Service Reporting [M1, M3, M18, M30] Section: 12.66 SIAM Introduction [M1, M5, M6, M10, M14, M30] Section: 12.68 SIAM Organisations [M1, M5, M6, M14, M29, M30] Section: 12.69 SIAM Operational Service [M5, M6, M29, M30] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.7
	30.2	Define and report on details of delivery of this capability and the measures of performance related to it within the Service Operations Manual.	
M31 Supporting the Authority Role	31.1	Where available as network packet payload information, provide access to usage statistics of externally hosted client Applications (including but not limited to web clients), services and components that interact with and/or impact the Services for up to 10 Authority (Tech Assurance) nominated staff.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.17 ITSM Tooling as a Tower Service [M1, M5, M6, M30, M31, M37] Section: 12.30 Availability Management [M1, M22, M30, M31]
	31.2	Provide dashboard delivered metrics on monthly, weekly and daily usage statistics for service utilisation.	

	31.3	Service information and dashboard delivered metrics to be available in real-time, in line with availability for the application being monitored, being those Non-Functional Requirements (as set out in Appendix 1 to this Annex).	
	31.4	Export and reporting capability to be provided for Authority to self-serve weekly or monthly period reports for offline consumption.	
	31.5	Where an application End User interface is delivered via a web browser these usage statistics should include (but not be limited to) the following: (a) browser make, version, Patch level; (b) screen size/resolution; (c) visit duration; and (d) operating system and version.	
	31.6	User initiated actions that result in Data exports and imports must include Data volumetrics for assessing volumes of Data being interfaced.	
M32 Technology	32.1	Ensure that all equipment utilised for the delivery of Services under Contractor control is sited, installed and maintained in accordance with 'Site Co-ordination and Installation Design Authority (SCIDA) Standards' unless agreed otherwise with the Authority (Tech Assurance).	Schedule 4.1 - Common Technical and Enabling Services Section: Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.57 Data Centre Services [M1, M32] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5, 16.6.8
	32.2	Complete and provide the Engineering Change Request (ECR) documentation for DAIS SCIDA approval, in accordance with the SCIDA standards and regulations.	
	32.3	Make available to the Authority (Tech Assurance) all Engineering Change Request (ECR) documentation within 2 Working Days of either receipt from, or submission to, DAIS SCIDA.	
	32.4	Change and configuration control of physical installations to conform to standards, including adherence to the Change Management Procedures.	
M33 Application Provisioning - Production	33.1	Provide, maintain, host, make available to the Authority, and support the Joint Personnel Administration system, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.59 Patching Services [M1, M24, M33, M38] Section: 12.88 Application

		(b) the functional requirements of the JPA business processes, as defined in this Agreement and the 'Business Process Guides'; (c) any Non-Functional Requirements relevant to JPA to be in accordance with the NFR Matrix (Appendix 1 of this Annex). For external End Users, Service availability to be measured at the MCN entry point; (d) all Patches for JPA to be applied in accordance with Patching requirements and timescales (Appendix 3 of this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5, 16.6.10
M34 Application Provisioning - Production	34.1	Provide, host, make available, maintain and support the 'Strategic MI (StratMI) System', which makes up the MP&VRP, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the StratMI Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to StratMI to be in accordance with the NFR Matrix (contained in Appendix 1 to this Annex); (d) all Patches for StratMI to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.54 IT Operations Management [M1, M22, M34,M35,M36] Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.77 SIAM Service Design [M1, M5, M6, M34] Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
M35 Application Provisioning - Production	35.1	Provide, host, make available, maintain and support the Agency Corporate Services System (ACSS) applications, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the ACSS business processes, as defined in this Agreement and the 'Business Process Guides';	Schedule 4.1 - Common Technical and Enabling Services Section: 12.54 IT Operations Management [M1, M22, M34,M35,M36] Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35,

		(c) the ACSS is comprised of the following database hosted application systems: (i) 'Armed Forces Memorial Database' (AFMD); (ii) 'Casualty Cell System' (CCS); (iii) 'Debt Management Database' (DMD); (iv) 'Gurkha Records Database' (GRD); and (v) 'Secretariat Business Database' (SECBUSDB); (d) any Non-Functional Requirements relevant to the ACSS to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex); (e) all Patches for the ACSS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); (f) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex); (g) User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS); and (h) provide a Volumetrics and End User report each week to the Authority (SO2 CASS).	M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	35.2	Provide and maintain an End User maintenance capability for ACSS, for creation, change and removal of End User accounts and the resetting of passwords.	
	35.3	Provide an electronic report of the volumetrics of End Users and all new End Users. The report is to also include the number of records held on this Application.	
M36 Application Provisioning - Production	36.1	Provide, host, make available, maintain and support the Compensation and Pension System (CAPS), in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the CAPS Business Processes, as defined in the Agreement and the 'Business Process Guides'; (c) extant technical specifications (as notified to the Contractor); (d) any Non-Functional Requirements relevant to CAPS to be in accordance with the NFR Matrix (Appendix 1 to this Annex). (e) all Patches for CAPS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex). (f) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to the Annex); and	Schedule 4.1 - Common Technical and Enabling Services Section: 12.54 IT Operations Management [M1, M22, M34,M35,M36] Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.75 SIAM Service Operations [M1, M5,M6, M13, M14, M25, M26, M34-M36] Section: 12.77 SIAM Service Design

		(g) User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	[M1, M5, M6, M34] Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	36.3	Provide an electronic report of the volumetrics of new and existing End Users to the Authority (SO2 CASS), including the number of records held on this Application.	
M37 Application Provisioning - Production	37.1	Provide, host, make available, maintain and support a Change Management System (CMS), in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the CMS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to CMS to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for CMS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.15 ITSM Tooling Transition to Existing Service [M1, M8, M9, M10, M28, M30, M31, M32, M37] Section: 12.16 ITSM Tooling Migration to Cloud [M1, M5, M6, M8, M9, M10, M30, M31, M37] Section: 12.17 ITSM Tooling as a Tower Service [M1, M5, M6, M30, M31, M37] Section: 12.40 Service Asset and Configuration Management [M1, M37] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.74 SIAM Process Responsibilities [M1, M5, M6, M14, M25, M26, M29,M37] Section: 12.76 SIAM Service Transition [M1, M5, M6, M14, M37] Section: 12.88 Application Provisioning – Production [M33-

			M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	37.2	Provide and maintain an End User maintenance capability for CMS, for creation, change and removal of End User accounts and the resetting of passwords to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	
	37.3	Provide an electronic report to the Authority (SO2 CASS) of the volumetrics of End Users and all new End Users. The report is to also include the number of records held on this Application.	
M38 Application Provisioning - Production	38.1	Provide, host, make available, maintain and support a Data Preservation Repository Reporting (DPRR) application, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the DPRR Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the DPRR to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the DPRR to be provided in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex); (f) User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS); and (g) Volumetrics and End User report provided each week to the Authority (SO2 CASS).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.56 Infrastructure and Software Management [M1, M23, M38] Section: 12.58 Anti-Virus (AV) Services [M1, M25, M38] Section: 12.59 Patching Services [M1, M24, M33, M38] Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5, 16.6.9 - 16.6.10
	38.2	Provide and maintain an End User maintenance capability for DPRR, for creation, change and removal of End User accounts and the resetting of passwords.	

	38.3	Provide an electronic report of the volumetrics of End Users and all new End Users. The report is to also include the number of records held on this Application.	
M39 Application Provisioning - Production	39.1	Provide, host, make available, maintain and support an 'Emergency Download of Contact Details' (EDCD) application, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the EDCD Business Processes, as defined in the Agreement and the 'Business Process Guides'; (c) any Non-Functional Requirements relevant to the EDCD to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the EDCD to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	39.2	Provide and maintain an End User maintenance capability for EDCD within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS), for creation, change and removal of End User accounts and the resetting of passwords.	
	39.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M40 Application Provisioning - Production	40.1	Provide, host, make available, maintain and support an Electronic Document Management (EDM) application, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the EDM Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the EDM to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the EDM to be in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

	40.2	Provide and maintain an End User maintenance capability for EDM within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS), for creation, change and removal of End User accounts and the resetting of passwords.	
	40.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M41 Application Provisioning – Production	41.1	Provide, host, make available, maintain and support a Far East and Nepal Administration System (FENAS) in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the FENAS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) FENAS is to be made available and accessible to the Nepal User community and locations (Kathmandu, Dharana, and Pokara); (d) any Non-Functional Requirements relevant to FENAS to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (e) all Patches for the FENAS to be in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (f) Incident Resolution in to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	41.2	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application;	
	41.3	Provide and maintain an End User maintenance capability for FENAS, for creation, change and removal of End User accounts and the resetting of passwords. End User account maintenance within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	
	41.4	Manage encryption key material for FENAS, including annual central key management for all sites in the UK and Nepal.	
	41.5	Attend Nepal site as required for incident resolution activities that cannot be reasonably undertaken remotely, which will be managed as non-Operational Change, and achieve Nepal site attendance incident resolution within 3 Working Days of arrival in Nepal.	
M42	42.1	Provide, host, make available, maintain and support a File Transfer System (FTS), in accordance with:	Schedule 4.1 - Common Technical and Enabling Services

Application Provisioning - Production		(a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the FTS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the FTS to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the FTS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	42.2	Provide and maintain an End User maintenance capability for FTS within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS), for creation, change and removal of End User accounts and the resetting of passwords.	
	42.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M43 Application Provisioning - Production	43.1	Provide, host, make available, maintain and support an Identity Card System (IDCS), in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the IDCS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the IDCS to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the IDCS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be actioned in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	43.2	Provide and maintain an End User maintenance capability for IDCS within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS), for creation, change and removal of End User accounts and the resetting of passwords.	

	43.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M44 Application Provisioning - Production		Provide, host, make available, maintain and support a JPA Portal to provide a means of disseminating information to the End User community by providing a message of the day capability, which can be altered on request by the Authority, in accordance with: (a) the latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); and (b) the functional requirements of the JPA Portal Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room, and additionally as: (i) JPA Portal to act as a single point of entry to JPA and provide links to other Services, including (but not limited to) 'Defence Learning Environment' and 'Defence Housing', and travel; (ii) message / information content to be updated on the JPA Portal within 1hr of the new content being issued by the Authority (Tech Assurance); (iii) JPA Portal to be available from MODNet connected End User devices and external networks; (iv) JPA Portal to have a flexible configuration capability to allow for additional hyperlinks and content to be added; and (c) any Non-Functional Requirements relevant to the JPA Portal to be in accordance with the NFR Matrix (Appendix 1 to this Annex). For external users, availability to be measured at the DBS ALI entry point; (d) all Patches for the JPA Portal in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex). (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
M45 Application Provisioning - Production	45.1	Provide, host, make available, maintain and support a Ministry of Defence Medal Office (MODMO) application, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support

		(a) the functional requirements of the MODMO Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (b) any Non-Functional Requirements relevant to the MODMO to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (c) all Patches for the MODMO to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (d) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Management (AMS) Paragraph: 16.6.5
	45.2	Provide and maintain an End User maintenance capability for MODMO, for creation, change and removal of End User accounts and the resetting of passwords. End User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	
	45.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M46 Application Provisioning - Production	46.1	Provide, host, make available, maintain and support a Prisoner Administration (PA) system., in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (a) the functional requirements of the PA Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (b) any Non-Functional Requirements relevant to the Prisoner Administration system to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (c) all Patches for the Prisoner Administration system to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (d) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	46.2	Provide and maintain an End User maintenance capability for PA, for creation, change and removal of End User accounts and the resetting of passwords. End User account maintenance to be actioned within 1	

		Working Day of receipt of an Authorised request from the Authority (SO2 CASS)	
	46.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M47 Application Provisioning – Production	47.1	Provide, host, make available, maintain and support a Veterans Welfare Computer System (VWCS), in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the VWCS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the VWCS to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the VWCS to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.88 Application Provisioning – Production [M33-M47] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	47.2	Provide and maintain an End User maintenance capability for VWCS, for creation, change and removal of End User accounts and the resetting of passwords. End User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	
	47.3	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application.	
M48 Application Provisioning - Support, Testing, Sandpit, Training	48.1	Provide, host, maintain and support a training Application Instance (Virtual Training Application Instance) for JPA HR Professional and Specialist Users., in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) training Application Instance software version shall be upgraded to reflect the current JPA Live and Strat MI systems within four weeks of change releases to either JPA or Strat MI, whichever is the	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]]

		latest, unless otherwise agreed with the Authority (Tech Assurance); (c) training Application Instance Data is to be refreshed at the request of the Authority (the trigger being when the data is no longer useable due to User entries) and completed and accepted by the Authority, within 2 Working Days); (d) manufactured synthetic data is to be used to comply with Data Protection Legislation; (e) any Non-Functional Requirements relevant to the VTE to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex) (f) all Patches for the VTE to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex). (g) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	48.2	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application;	
M49 Application Provisioning - Support, Testing, Sandpit, Training	49.1	Provide, host, maintain and support a training Application Instance for JPA Prisoner Administration Users, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) training Application Instance software version shall be upgraded to reflect the current JPA Live and Strat MI systems within four weeks of change releases to either JPA or Strat MI, whichever is the latest, unless otherwise agreed with the Authority (Tech Assurance); (c) Training Application Instance Data is to be refreshed at the request of the Authority (SO1 C&I). (the trigger being when the data is no longer useable due to User entries) and completed and accepted by the Authority (SO1 C&I), within 2 Working Days; (d) manufactured synthetic data is to be used to comply with Data Protection Legislation; (e) any Non-Functional Requirements relevant to the JPA Prisoner Admin training Application Instance to be in accordance with the NFR Matrix (Appendix 1 to this Annex);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

		(f) all Patches for the JPA Prisoner Admin training Application Instance to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (g) Incident Resolution to be performed in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	
	49.2	Provide an electronic report of the volumetrics of End Users and all new End Users each week to the Authority (SO2 CASS). The report is to also include the number of records held on this Application;	
M50 Application Provisioning - Support, Testing, Sandpit, Training	50.1	Provide JPA E-Learning Training for HR Professional and Self Service Users, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) e-Learning material to be updated to reflect all changes of each major JPA release within 4 weeks of each major JPA release, unless agreed otherwise by the Authority (SO1 C&I); (c) e-Learning material to be made available on the JPA Portal and passed by electronic media to the Authority; (d) e-Learning material must be compatible with being hosted on the MOD Defence Learning Environment. (e) training coverage to include, but not be limited to the following business function areas: (i) HR Professional; (ii) Self Service and Career Manager; (iii) Absences; (iv) Appraisals; (v) Pay; (vi) Expenses; (vii) Disturbance & Education; (viii) Early Termination; (ix) Service History; (i) Personnel Details; (f) any Non-Functional Requirements relevant to the JPA e-Learning Training Application Instance to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex); (g) all Patches for the JPA E-Learning Training Application Instance to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

		(h) Incident Resolution to be performed in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	
M51 Application Provisioning - Support, Testing, Sandpit, Training	51.1	Provide, host, make available, maintain and support a VWCS training application, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) the functional requirements of the VWCS Business Processes, as defined in the Agreement and the 'Business Process Guides' available in the Data Room; (c) any Non-Functional Requirements relevant to the VWCS to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the (VWCS) to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex); and (e) Incident Resolution to be performed in accordance with the Incident Resolution Matrix (Appendix 2 to this Annex).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5
	51.2	Provide and maintain an End User maintenance capability for the VWCS Training application, for creation, change and removal of End User accounts and the resetting of passwords. End User account maintenance to be actioned within 1 Working Day of receipt of an Authorised request from the Authority (SO2 CASS).	
M52 Application Provisioning - Support, Testing, Sandpit, Training	52.1	Provide host, make available for use by the Authority by July 2020, maintain and support a JPA and StratMI SandPit Application Instance, in accordance with: (a) latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (b) all Changes (including patching) to be applied to the Application Instance no more than 2 weeks after the live Application Instances are updated, to ensure the currency of functionality is close to the extant production Application Instance; (c) any Non-Functional Requirements relevant to the JPA and StratMI Sandpit Application Instance to be provided in accordance with the NFR Matrix (Appendix 1 to this Annex); (d) all Patches for the JPA and StratMI Sandpit Application Instance to be applied in accordance with Patching Requirements and Timescales (Appendix 3 to this Annex);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

		(e) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 of this Annex); (f) the user interface to the Application Instance shall include a persistent, clear and unambiguous identification mechanism to distinguish it from the Production instance; and (g) the Application Instance shall have all functionality of the live JPA/OBIEE system, including (but not limited to): (i) print; (ii) workflow; (iii) exporting OBIEE and concurrent report data to excel; (iv) capability for Authority staff to develop and amend OBIEE reports; and (v) security features and accreditation in line with the live system.	
M53 Application Provisioning - Support, Testing, Sandpit, Training	53.1	Ensure that the JPA & StratMI sandpit Application Instance meets the Authority functional and data requirements, in accordance with: (a) the Application Instance requiring ID verification details and sexual orientation declaration data items to be amended/anonymised (as directed by SO1 Pers Processes); (b) the data set for the Application Instance being reflective of the production Application Instance in volume, construct, and content; (c) the Application Instance having the same JPA/StratMI responsibilities and Security Profiles as those allocated in the live system except for the Authority Process Leads who require the JPA responsibility of TAS System Admin; (d) MI staff requiring access to change permissions on the 'Mil MI Administration Tool to manage catalogue groups'; (e) the personnel data in the Application Instance to be refreshed in line with Release updates, CMUs, Fixes and Patches; (f) successfully process JPA Application Instances running overnight and processes successfully; (g) Application Instance being kept up to date; Release updates, CMUs, Fixes and Patches must be applied to the system in line with the live instance of JPA and Strat MI which includes the EOY/SOY processes; (h) an ETL to populate the StratMI element of the Application Instance, to be run to the same frequency as Production to update the OBIEE Strat MI data, unless otherwise agreed with the Authority and overnight ETL status to be communicated to a group email maintained by the Authority;	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

		(i) an update to OBIEE Strat MI WebCat (taken from live JPA) to run every 28 days to maintain currency of the OBIEE Strat MI folder structure; and (j) the Application Instance benefitting from a technical helpdesk support (JPAC EC), BPO support, JPA and StratMI system support and administration.	
M54 Application Provisioning - Support, Testing, Sandpit, Training	54.1	Provide Application Instances to the Authority (Test Manager) capable of undertaking User Acceptance Testing (UAT) of Releases and change, to enable meaningful and representative testing in alignment with the following, unless agreed otherwise by the Authority (Test Manager): (a) must meet the detailed requirements as set out in Schedule 6.2 (Testing), and Schedule 8.2 (Change); (b) must meet the criteria as agreed in the Test Plan for the Release or change being tested; (c) Application Instances(s) to be made available to the Authority, with the fully deployed Release or change content, at least 10 Working Days prior to the commencement of UAT; (d) Application Instance(s) availability and data content (Release or change dependent) will be established as entry criteria for the UAT and agreed by the Authority within the Test Plan; (e) for the duration of the UAT phase and the pre and post availability periods, the Application Instance(s) are to be for the exclusive use of the Authority; (f) the UAT duration must be agreed by the Authority (Test Manager) in the Test Plan but will be defaulted to 10 Working Days for a Major Release; (g) Application Instances(s) to be retained and remain available to the Authority, for at least 10 working days following the deployment to Production of the Release or change; (h) to be capable of undertaking testing of all Business Processes and their dependent Applications in scope of the Release or change being deployed; (i) capable of representative testing of the Release or change being deployed, as it will be subsequently applied to Production; (j) where testing requires interfacing or integration of more than one Application then that technical and functional capability is to be available;	Schedule 4.1 - Common Technical and Enabling Services Section: 12.55 Application Provisioning - Support, Testing, Sandpit, Training [M1, M34, M35, M36, M48, M49, M50, M51, M52, M53, M54] Section: 12.90 Application Provisioning - Support, Testing, Sandpit, Training [M48-M54]] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.5

		(k) Application Instance(s) will be populated with live data (non-obfuscated) unless agreed otherwise with the Authority (Test Manager); (l) currency of data in the test Application Instance(s) to be no older than 20 Working Days from the start date of UAT; (m) data integrity, currency and consistency must be maintained across all Application Instances(s), where integration and interfacing is being tested; (n) Application Instance(s) to be accessible from Authority End User access devices; (o) Applications to be provided in accordance with latest approved version of the technical specifications (identified and referenced in the "Apps Design Docs Matrix" that is held in the Data Room); (p) UAT Application Instance(s) to have sufficient capacity to conduct full end-to-end testing during the UAT phase without unreasonable limit on the number of testers; (q) UAT Application Instances(s) to be representative of the performance and capability on the equivalent Production Application Instances for all End User interface activities; (r) provide UAT End User access accounts to the Authority (Test Manager) 10 Working Days in advance of UAT commencement; (s) where the Mil Pers & Vets Reporting Platform is being tested, the Application Instances(s) must be capable of executing Data Warehouse Initial Load and Incremental Load tests for full data lifecycle testing from source Application Instance(s) to Data Warehouse; and (t) any Non-Functional Requirements relevant to the UAT Application Instance(s) to be accordance with the NFR Matrix (Appendix 1 of this Annex) and all downtime/unavailability of the Application Instance(s) must be agreed with the Authority (Test Manager).	
M55 Interface Provisioning	55.1	Deliver, maintain and support all Data interfaces (both intra and inter the IT Environment), in accordance with: (a) the latest approved version of the technical specifications (identified and referenced in "The Data Interfaces Register" held in the Data Room); (b) the current set of interfaces as listed in the "The Data Interfaces Register" (held in the Data Room); (c) create and maintain an Interface Control Document for all Data Interfaces and Data Feeds which is to be agreed between the	Schedule 4.1 - Common Technical and Enabling Services Section: 12.4 Service Asset and Configuration Management [M1, M37] Paragraph: 12.40.2

		sending and receiving parties and the Authority (Tech Assurance) and provided to the Authority within 10 Working Days of issuing the final agreed version; (d) Data Interface errors (for example, but not to be limited to; data issues, communications issues, logic issues, technical / functional errors, off schedule runs) must be reported to the Service Desk for investigation, resolution or progression; (e) a weekly Data Interfaces status report to be provided to the Authority (Tech Assurance) on the first Working Day of the week, to cover the period since the last report was delivered. The report must include, but not be limited to; (i) report on all executions of all Interfaces & Data Feeds; (ii) date & time of each execution - start and end times; and (iii) status of execution (for example, fail, completed no errors, and stalled); and (f) data volumes for success and fail (row count and/or Mb). Each scheduled report has a specific criterion in relation to the date and the frequency it is run. Examples of these reports are found in the Data Room. Currently these are Interface Error Reports for DMICP and DRS. (a) any Non-Functional Requirements relevant to the Data Interfaces and Feeds to be in accordance with the NFR Matrix (Appendix 1 to this Annex); (b) all Patches for the 'Data Interfaces' and 'Feeds' to be applied in accordance with Patching Requirements and Timescales (Appendix 3 of this Annex); and (c) Incident Resolution to be provided in accordance with the Incident Resolution Matrix (Appendix 2 of this Annex).	
	55.2	For the avoidance of doubt, 'Interfaces' includes all electronic and non-electronic transmission of structured data, regardless of the underlying platform used to export, import or interface the Data (i.e. it is not solely the hub based interfaces).	
M56 Data Room	56.1	Within 60 Working Day of the Effective Date, undertake an audit on the Data Room and perform the following: (a) identify all necessary and valid documentation; (b) ensure all valid documentation is consistently formatted to templates agreed with the Authority; (c) relocate identified documentation to the future Data Room structure; and	Schedule 4.1 - Common Technical and Enabling Services Section: 1.1 Introductions and Solution Overview Paragraph: 1.1.3

		(d) archive all documentation identified as retired.	
M57 Data Room	57.1	Every 2 months from Effective Date, provide a copy of the Data Room in the format as agreed between the Parties.	Schedule 4.1 - Common Technical and Enabling Services Section: 1.1 Introductions and Solution Overview Paragraph: 1.1.3
M58 Data Room	58.1	Within 3 months from Operational Service Commencement Date, update the Service Operation Manual to establish the process and procedures for maintaining, auditing and refreshing the Data Room which shall include the following obligations: (a) maintain a comprehensive, coherent and valid copy of the full set of technical and business process documents that define and document the Services and their provision; (b) the Data Room must contain all documentation that is maintained by the Contractor to support the provision of the Services; (c) the Data Room must be structured and matured based upon ITSM stages and must accommodate the disaggregation of the Services and the needs of the Pseudo SIAM approach; (d) from Operational Service Commencement Date, provide a refresh every two months to the Business Continuity Data Room, such that it fully reflects the complete content of the Contractor documentation at that time; and (e) provide any reasonable assistance to the Authority to allow for an audit of the Data Room to be undertaken by the Authority following each refresh.	Schedule 4.1 - Common Technical and Enabling Services Section: 1.1 Introductions and Solution Overview Paragraph: 1.1.3
Schedule 2.1, Part 15 (Technology)			
INTRODUCTION	2.1	This Part 15 to Schedule 2.1 sets out the Authority's requirements, in relation to: (a) Transition Services (including Transformation) for Technical Infrastructure; (b) Technical Refresh to comply with Evergreen requirements; (c) hosting, Hardware and Software obligations regarding licensing, technology management and configuration management; (d) the DBS Mil Pers & Vets Design Standards and Principles; and (e) technology back-up requirements.	

	2.2	The related Performance Levels are set out in Part 13 of Schedule 2.1 (Service Requirements – IT Service Management), Schedule 2.2 (Performance Levels), and Annex M (Technology and IT Services).	
SERVICE CHANGE & SERVICE DESIGN	3.1	The Contractor understands that the Technical Infrastructure may be the subject of upgrade, renewal, or replacement during the Term to allow the Contractor to continue to deliver the Services and undertake Transformation. If the Authority requires the Contractor to make any other change to the Technical Infrastructure this shall be dealt with in accordance with the Change Control Procedure. This Paragraph sets out the: (a) basis on which the Contractor may make changes to the Technical Infrastructure as Operational Changes; (b) the Authority Requirements for Technical Refresh to maintain Evergreen state; and (c) Transformation activities to support the Transformation Requirements set out in the Detailed Transformation Plan, contained in Schedule 6.1 (Transition and Transformation Plan).	Schedule 4.1 Organisation and Governance Section: 7.5 Change Initiation, Impact and Approval/Rejection
	3.2	The Contractor shall: (a) only be entitled to make changes to the Technical Infrastructure in accordance with the agreed Architecture Management Procedures and the Change Control Procedure; (b) when planning or implementing any changes to the Technical Infrastructure, work collaboratively with the Authority in accordance with: (i) the Architecture Management Procedures and the Joint Architecture Governance framework; and (ii) if necessary, the Change Control Procedures to ensure that plans relating to changes to the Technical Infrastructure are integrated and coherent with the overall change programme and plans; (c) maintain the Technical Infrastructure providing the Services with an Evergreen state by doing the following: (i) refreshing all Hardware components of the Technical Infrastructure at least once during the Initial Term (excluding the Authority Communications Infrastructure and MODNet (or equivalent) connected End User accessed devices (save those devices provided to the Contractor for use by the Contractor);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.7 Architecture and Operations Governance. Section: 7.5 Change Initiation, Impact and Approval/Rejection

		(ii) ensuring that the Software is within a single release of the current approved version (known as n-1), unless otherwise agreed with the Authority, with a clear upgrade or migration path identified, running on a sufficient and capable platform throughout the life of the Agreement and capable of supporting the provision of the Services in accordance with the requirements set out in the Agreement for a minimum of 2 years after the expiry or termination of this Agreement. Either Party may make a written recommendation to the other that it is not in the interests of the Authority to undertake such an upgrade so as to conform with this requirement; (iii) ensuring that all ICT used to deliver the Services is fully supportable (with all necessary security, legal or core functional Updates and Patches) by the ICT vendor or a vendor authorised third-party, for a period of 2 years after the Expiry or Termination of this Agreement; and (iv) specifying the Technical Refresh commitment on a Change Authorisation Note adding any Hardware and Software components to the Technical Infrastructure and notified such commitments, when agreed between the Parties, against the items on the Configuration Management Database; (d) notwithstanding the above Paragraph 3.2(c) (unless otherwise agreed in writing by the Authority): (i) identify and, with the Authority's agreement, implement appropriate alternatives in the event that they are aware any Software and Hardware will or may be declared obsolete by the third party vendor (for example, where such Software and Hardware is announced to be at its terminal release or has no viable future upgrade roadmap at the termination of the Agreement); (e) undertake planning and design determinations for Evergreen adherence, which includes the latest vendor software product release and support characteristics which shall factor in a higher frequency of application update release cycles and/or alternative deployment mechanisms into future Evergreen planning; and (f) replace peripheral equipment (supplied by the Contractor to deliver the Services) as reasonably required in order to maintain the functionality of equipment at or close to accepted industry standards as	

		agreed by both Parties and in any event at least once during the period from the Effective Date for the remainder of the Initial Term.	
	3.3	Where any Application (for which the Contractor is not responsible) is already installed then the Contractor shall reinstall the Application as part of any Technical Refresh process, after undertaking the appropriate due diligence analysis to establish the validity of the Application being reinstalled.	
	3.4	Where the Technical Refresh carried out under Paragraphs 3.2(c) and 3.2(f) contains enhanced functionality as part of the standard product, the enablement of such enhanced functionality will not be the subject of an additional charge by the Contractor.	
TECHNOLOGY ROADMAP	4.1	The Contractor understands that the Authority is engaging with it to ensure that the Hardware and Software underpinning the delivery of the Services (save for the Authority Communications Infrastructure) is upgraded and refreshed during the Term, in order to ensure that: (a) such Hardware and Software is capable of delivering the Services (throughout the Term) in accordance with the provisions of the Agreement; (b) the Contractor hands over a 'viable service' upon expiry or termination of this Agreement (i.e. the Hardware and Software is capable of being supported for a period of 2 years post expiry of the Agreement); and (c) the Authority transformation needs for the services and technology adhere to the Service Transformation Strategy, as regards application transformation and technology and service disaggregation.	Schedule 4.1 - Common Technical and Enabling Services Section: 11 Evergreening Section: 12.22 Service Strategy [M1, M15] Section: 8 Software and Licensing Section: 12 Service Management and ITSM
	4.2	The Contractor shall: (a) produce, maintain and make available to the Authority a detailed Technology Roadmap of Hardware and Software, for the Term and 2 years thereafter, to show the complete set of Technical Refresh activities of all Hardware and Software components; (b) provide support to the Authority, as part of the Joint Architecture Governance framework, in creating an Authority owned and maintained rolling 10-year Technology Roadmap; and (c) carry out the Technical Refresh in accordance with Schedule 4.1 (Contractor Solution), which is the Contractor Solution for delivering the Services Transformation as specified by the Service Transformation Strategy.	

SERVICE OPERATION MANAGEMENT & SERVICE DESIGN Capacity Management	5.1	The Contractor shall: (a) continually seek to reduce costs associated with the Contractor System by reducing the size and scale of the ICT landscape (including, but not limited to, consolidating, rationalising, simplifying product usage and adoption of alternative solutions through the use of thin provisioning, multi-tenanting, and ICT housekeeping measures); (b) provide the scalability characteristics (including but not limited to storage, bandwidth, compute and memory) of the ICT landscape of the Contractor Solution, which must be made available as costed and fully defined elements of the Service Catalogue; (c) provide and maintain storage capacity and capability that provides for the established growth projections of the Services; and (d) provide evidence of such cost-saving actions performed under this Paragraph 5.1, as identified in the Capacity Management Reports.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.12 ITSM Transformation (Evolve to Pseudo SIAM) [M1, M5, M6, M29, M30] Section: 12.13 Full Disaggregation and Pseudo-SIAM [M1, M5, M6] Section: 12.62 Continual Service Improvement [M1, M11] Section: 12.71 SIAM Process [M1, M5, M6, M11, M14, M26] Section: 12.72 SIAM Organisation Model [M1, M5, M6, M11, M14, M25, M37] Section: 12.23 Demand Management [M1, M20] Section: 12.31 Capacity Management [M1, M20] Section: 12.42 Software Asset and Licence Management [M1, M20]
Data Centre Facilities	5.2	The Contractor shall: (a) unless agreed by the Authority, ensure that all Data Centre facilities used to deliver the Services are Authority-owned or, if not Authority-owned, compliant with Tier 3 and List X; (b) ensure power, space, security and HVAC requirements within all Contractor Premises hosting ICT equipment are maintained and optimised to meet current requirements and have consideration to planned change in line with the Technology Roadmap; (c) fund and resource activities resulting from both planned and unplanned system downtime and outages impacting on the delivery of the Services; (d) host the Disaster Recovery environment within a separate Site to the Production Environment;	Schedule 4.1 - Common Technical and Enabling Services Section: 12.57 Data Centre Services [M1, M32]

		(e) ensure that the Contractor administration of delivered services is not impacted by planned outages of Authority or any third party Networks (where services are not hosted in Authority data centres); (f) where possible, use Data Centres and Cloud Hosting which are capable of operating unmanned and/or with autonomous processes during both core and non-core hours and, where these processes need to be monitored remotely, the Contractor shall ensure delivery of the Services is not impacted by planned Network outages impacting Authority or any third party Networks; and (g) provide support to third parties undertaking testing and maintenance tasks in locations where DBS Mil Pers Technical Infrastructure is located but suitable resources are not based on site including, but not limited to: (i) electrical testing in accordance with the 'Electricity at Work Regulations'; (ii) the servicing or replacement of HVAC requirements within in Data Centres and Network rooms; (iii) provide escorted access to Data Centre cages; (iv) the power down and up of Data Centre or Network room Hardware as required; and (v) works services, upgrades, maintenance and testing.	
Site Co-ordination and Installation Design Authority Standards (SCIDA)	5.3	The Contractor shall: (a) ensure that the Contractor System is sited and installed in accordance with SCIDA standards; (b) propose and implement TEMPEST countermeasures to conform to standards and be approved by the Authority prior to implementation; and (c) where applicable, complete the Engineering Change Request documentation and submit for approval by DAIS.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.57 Data Centre Services [M1, M32]
Authority to Operate for Services	5.4	The Contractor shall: (a) ensure that the Contractor System meets the policy and accreditation mandates of the Authority to be granted an Authority to Operate; (b) for all ICT, ensure that the hosting platforms utilised in this Agreement are: (i) able to access the Services via an accredited route that is compliant with JSP 604 (for example, MCN through SDP or SMI gateway);	Schedule 4.1 - Common Technical and Enabling Services Section: 12.57 Data Centre Services [M1, M32]

		(ii) accredited and holding Authority to Operate in compliance with JSP 604 and utilise the risk-appropriate security measures for information at 'OFFICIAL-SENSITIVE' or higher classification in accordance with the 'Government Security Classification' and associated documentation (as amended and updated from time to time); (iii) maintained and supported by undertaking all necessary data centre activities related to the maintenance of data centre power, space and HVAC requirements; and (iv) maintained and supported in line with rest of the ICT, in accordance with the corresponding Service Requirements contained in Annex M (Technology and Applications).	
Maintain all Information and Communications Technology	5.5	The Contractor shall: (a) maintain all ICT used to deliver the Services with support arrangements which ensure the Service adheres to the stipulations of the Authority to Operate, security accreditation and Evergreen requirements; (b) support and adhere to the Authority's policy for reducing the overall carbon footprint and use of resources by mandating the procurement and use of energy-efficient ICT contained in DIN 2011 DIN06-008, whereby the Contractor is required to consider the sustainability criteria when purchasing or developing ICT equipment, solutions or services, including: (i) 'direct effect', being the change in resource consumption between old and new equipment; (ii) 'indirect effect', being the impact on the overall resource consumption of the business processes supported by ICT; (iii) 'procurement effect', being the resource consumption involved in the change (such as design, manufacturing and disposal, or relocation and termination of services); and (iv) 're-use', where the energy consumption and carbon emissions of the older ICT equipment are consistent with the intent of this policy then consideration must be given to the re-use of available ICT equipment in meeting the requirement; (c) create and maintain a Patch management strategy for the Technical Infrastructure used to deliver and support the Services, to include the following:	Schedule 4.1 - Common Technical and Enabling Services Section: 11 Evergreening Section: 12.22 Service Strategy [M1, M15] Section: 1.1 Application Support Management (AMS)

		(i) all Hardware and Software Patching is to be kept up to date and implemented in accordance with the patching requirements and timescales as detailed in Appendix 3 of Annex M (Patch Requirements and Timescales); (ii) monitor the deployment status for Patches for all networked and non-networked ICT; (iii) impact assessment, Testing and implementation of Patches to be in accordance with the Change Control Procedures; (iv) maintain an audit and history record of Patches, to be made available to the Authority on request; (v) review all MODCERTS and deploy Patches, or take other appropriate actions, to address the documented vulnerabilities identified; and (vi) source Patches from DOBUS or where not available, from vendor websites; and (d) implement Anti-Virus Software updates across all ICT systems used to deliver and support the Mil Pers & Vets services, including: (i) Anti-Virus Software Patching and Anti-Virus Software database updates are to be kept up to date and implemented in accordance with the patching requirements and timescales as detailed in Annex M (Technology and Applications); (ii) monitor the deployment status for Anti-Virus Software updates for all networked and non-networked ICT; (iii) impact assessment, Testing and implementation of Anti-Virus Software Patches and database updates to be in accordance with the Change Control Procedure; (iv) where it is not technically feasible or advisable to implement, the Authority must be notified immediately; and (v) Anti-Virus Software updates to be sourced from DOBUS or where not available, from vendor websites.	
Migration to Cloud	5.6	When producing the Transformation Plan in accordance with Part 2 Schedule 6.1 (Transition and Transformation Plans), the Contractor shall detail how all existing applications and technology used for the Services will be migrated to Cloud (or a hybrid-Cloud) services utilising 'Infrastructure as a Service' as the minimum level (unless otherwise agreed by the Authority).	Schedule 4.1 - Common Technical and Enabling Services Section: 5 Cloud Migration Approach

	5.7	For the avoidance of doubt, where the Authority refers to a requirement for Cloud, the Authority is seeking the following characteristics from such a solution: (a) a well-defined catalogue of Technical Infrastructure, Platform and Software service options; (b) pricing (seeking an overall cost reduction) on a utility computing basis and 'fine-grained' or modularised with usage-based billing options for all service variants (for example, Technical Infrastructure tiers, platform management options, application options, availability, and security levels); (c) high levels of scalability (agile, flexible and responsive), with capabilities that can be elastically provisioned (in some cases automatically) to scale rapidly outward and inward commensurate with demand; (d) high levels of automation and orchestration of tasks and processes (leading to flexible and rapid provisioning with lower costs); (e) mature ITSM across all areas; (f) mature security controls (appropriate to the requirement); (g) abstraction from maintenance, insulating the Authority from the need to additionally consider and fund Evergreening of underlying service components (for example, ICT and datacentre facilities); (h) high levels of reliability, evidenced through mature service level reporting; (i) mature business continuity and disaster recovery measures (low recovery times) and options for Recovery Time Objectives and Recovery Point Objectives; (j) high levels of portability to relocate technology/application components to alternative hosting platforms in the future with relative ease with no cost penalty (Cloud native applications); (k) application solutions must be Cloud native releases which are transportable and modularised; (l) platforms which are Cloud native (for example, the Services should have a platform agnostic in relation to the underlying operating system) offering maximum portability between Application Instances, based on a containerisation and build script automation approach); and (m) adoption of hybrid solutions, due to complexity of customisations of COTS products must be considered, to allow for a staged Transition and Disaggregation of the Services.	

Access to Contractor Hosted Services & Tooling	5.8	The Contractor shall: (a) make available to the Authority or embedded Contractor Personnel the Contractor provided tools, services, and resources at the individual's regular place of work and utilising the Authority provisioned End User access device on the Authority's Network, in line with any and all specific requirements detailed with this Agreement; (b) up to 6 months from the Operational Services Commencement Date, enable access to End Users via Contractor provided devices (with prior agreement of the Authority) and, where Contractor provided devices are provisioned, they must have the following capabilities available for use: (i) comply with all requirements within Annex M for the delivery of ICT in terms of JSP604 and JSP440 compliance; (ii) be connected to the MCN; (iii) have, as a minimum, Microsoft Office Standard (including Microsoft Outlook) and Internet Explorer and any other software to enable the required connectivity; (iv) host an End User profile; (v) allow End Users to log on from any device on the Contractor managed Network; (vi) host a working messaging service for internal and external e-mail; (vii) provide access to approved internet hosted websites; (viii) provide access to File storage (Personal and Shared); and (ix) support provided via the Service Desk; and (c) within 6 months from the Operational Services Commencement Date: (i) provide and maintain access by End Users to Contractor hosted services and tooling provided via Authority MODNet devices; and (ii) perform user identity and access management.	Schedule 4.1 - Common Technical and Enabling Services Section: 11 Evergreening Section: 12.22 Service Strategy [M1, M15]
	5.9	**Access to Third Party Software vendor support services** (a) The Authority acknowledges and understands that Third Party Software vendors such as Oracle have a rich source of information available on their support websites, which will be pertinent to the Technical Assurance capability of the Authority which they shall make available to Authority staff. **Access to be provided**	Schedule 4.1 - Common Technical and Enabling Services Section: 12.54 IT Operations Management [M1, M22, M34,M35,M36]

		(b) The Contractor will provide access to the Third Party Software vendor support services, where this is not prohibited by commercial agreements in place between Contractor and such third party, across all applications and technology stack that are used to deliver the Mil Pers & Vets services. Such access is to include, but not be limited to: (i) ability to view active and historical service requests or problem records for the Mil Pers & Vets services; and (ii) ability to view any Third Party Software vendor knowledge or training materials pertinent to the service provision. **Fall-back alternatives to direct access** (c) Where the Contractor is unable to provide direct access to the Third Party Software vendor support services, due to commercial agreements in place between Contractor and such third party, the Contractor will provide, on request, a technically unexpurgated report of the detail regarding service requests or problem records related to the Mil Pers & Vets services.	
DBS DESIGN STANDARDS AND PRINCIPLES	6.1	All Contractor produced design materials, testing scope, tools, applications, operational processes and service delivery shall evidence the adherence to and implementation of (unless agreed otherwise with the Authority) the design standards and principles as contained within DBS Mil Pers & Vets Design Standards & Principles.	Schedule 4.1 - Common Technical and Enabling Services Section: 12.9 12.9 Architecture strategy and portfolio Paragraph: 12.9.14
	6.2	The DBS Mil Pers & Vets Design Standards & Principles does not override or make redundant any Standards contained in Schedule 2.3 (Standards).	
	6.3	The Contractor is required to input to and enhance the DBS Mil Pers & Vets Design Standards & Principles document, to drive benefit for the Parties which shall be triggered by (but not limited to) the following events: (a) changes to industry best practice; (b) changes to technology trends; (c) issue or up-issue of vendor roadmap or direction statements; and/or (d) Mil Pers & Vets change deployments.	
	6.4	The Authority shall maintain the DBS Mil Pers & Vets Design Standards & Principles document and any changes to it during the Term shall be subject to approval by the Joint Architecture Board.	

INFORMATION TECHNOLOGY BACK-UP AND RESTORE	7.1	The Contractor shall, no later than 30 Working Days prior to the Operational Service Commencement Date, provide a draft Back-Up Plan for approval by the Authority. The draft Back-Up Plan shall be based on Paragraph 7.5 below and the existing Back-Up Plans (which will be provided to the Contractor on request).	Schedule 4.1 - Common Technical and Enabling Services Section: 12.59 Patching Services [M1, M24, M33, M38] Section: 12.60 Backup Services [M1, M24] Section: 1.1 Application Support Management (AMS) Paragraph: 16.6.10 - 16.6.11
	7.2	The Parties shall ensure that the draft Back-Up Plan is agreed no later than 10 Working Days following the Operational Service Commencement Date.	
	7.3	The Contractor shall: (a) maintain the Back-Up Plan throughout the Term and shall ensure that the Back-Up Plan is executed in accordance with its provisions on and from the Operational Service Commencement Date; (b) ensure that the Back-Up Plan is fully reviewed and if necessary updated, during Impact Assessments and design work undertaken as part of the Change Control Procedure; and (c) back-up all Data and on a regular basis (initially utilising the agreed incremental, full, and archive back-up strategy), following the applicable technical Standards and in accordance with the agreed Back-Up Plan, to meet the following: (i) ensure that the Disaster Recovery requirements of the Service are met (as contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability)); (ii) Authority Data must be retained, secured and disposed of in adherence to the requirements of the DBS Retention and Disposal Schedule; and (iii) all other Data which does not constitute Authority Data, but upon which the Contractor Systems are dependent in order to deliver the Service, must be backed up alongside the Authority Data; and (d) each Quarter perform a full restore and recovery test of the back-up capability to test that the technical and procedural processes in place are sufficient to undertake a full data back-up and restore (including all of the Authority Data) in accordance with the requirements of the Bank-Up Plan and, within 10 Working Days, provide to the Authority a report	

		evidencing performance and successful completion of such test against the requirements of the Back-up Plan.	
	7.4	Should it be necessary, the Contractor shall: (a) perform any data restore (including all of the Authority Data) within the time periods set out in the Back-Up Plan (to reflect the time periods contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability); (b) keep the Authority updated with regard to the restoration of data; and (c) the time period shall be measured from the start of the relevant incident that triggered the recovery requirement, including where it is necessary for the Contractor to use data back-ups stored in a secure off-site location.	
	7.5	The Back-Up Plan shall contain the following minimum requirements: (a) the scope of the back-up strategy to include all storage components that encompass the Contractor Systems (to become Appendix 1 to the Back-Up Plan), being: (i) the primary focus and detail required in the plan will be on the Authority accessed Production Environment; and (ii) ICT within the Development Environments, Production Environment, and DR environment that make up the Service, but which are not Authority facing, must also be included in the Back-Up Plan; (b) procedures setting out how the Contractor will regularly perform incremental data back-up operations of the Hardware set out at Appendix 1 of the Back-Up Plan sufficient to ensure the Contractor is able to comply with the data restore timescale in Paragraph 7.4 above (Incremental Back-Up); (c) procedures setting out how the Contractor shall regularly perform a full data back-up operation of the Hardware set out at Appendix 1 of the Back-Up Plan on Friday of each week sufficient to ensure the Contractor is able to comply with the data restore timescale in Paragraph 7.4 above (Full Back-Up); (d) procedures setting out how the Contractor shall perform a full, verified, data back-up operation of the Hardware set out at Appendix 1 of the Back-Up Plan on the last working day of each month (Archive Back-Up);	

		(e) in the event of a critical change (as agreed by the Contractor and the Authority on a case by case basis) to the software application code create a full, verified back-up to back-up media; (f) ensure the back-up media used by the Contractor to create the data back-up contains no information or data other than the Authority's related back-up data and information including the Authority Data; (g) ensure that Authority Data (in whatever form) is not available to, or accessible by, any third parties except those to whom the Authority grants permission and those Sub-Contractors permitted to access the Authority data by the provisos of this Agreement; (h) implement processes to transport securely and confirm in writing, the back-up of the Authority data to and from the secure off-site location approved by the Authority; (i) ensure that the recording of Authority Data on all data back-up tapes (used for off-site data storage) is verified as successful and complete prior to such back-up media being despatched to the approved secure off-site location; (j) ensure that the secure off-site storage facilities used for the back-up media containing Authority Data are located at sites deemed suitable after comprehensive threat assessments taking into account security, access/logistics, sustainability, distance from the master copy of the Authority Data and environmental conditions; (k) the detailed restore and recovery process documents, referenced from the Back-Up Plan and made available to the Authority and detail the steps to be taken to recover and restore all Authority Data; (l) ensure that data integrity and coherence of Data is maintained for all back-ups; (m) a non-intrusive and non-destructive data recovery capability is required, at both whole and record level granularity; (n) ensure that data back-ups are stored at the approved secure off-site storage facility; (o) ensure there is no unauthorised access to the data back-ups stored at the approved secure off-site storage facility; (p) unless agreed otherwise with the Authority, ensure that: (i) the Incremental Back-Up is stored for a period of not less than 24 hours (from when the back-up was taken);	

		(ii) the Full Back-Up is stored for not less than 28 days (from when the back-up was taken); and (iii) the Archive Back-Up is stored for not less than 52 weeks (from when the Back-Up was taken); (q) comply with the BCDR Plans to enable the Contractor, within the RPO and RTO times (contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability)), from the start of the relevant incident, to take data back-ups stored off-site and reconstruct the relevant systems (hosting the Authority data) at an alternative location and continue to provide the Services and the Authority Data in accordance with this Agreement from such alternative location.	
Schedule 2.4 – (Security Management)			
INTRODUCTION	1.1	The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Authority Premises and data (including Authority Data).	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.2
	1.2	The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Agreement will be met.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.5
	1.3	The Contractor shall appoint a member of the Portfolio Management Board to be the Contractor Account Security Manager.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.3
	1.4	The Authority shall appoint a member of the Portfolio Management Board to be the Authority Security Officer.	
	1.5	The initial member of the Portfolio Management Board appointed by the Contractor for such purpose shall be the person named as such in Schedule 9.2 (Key Personnel) and the provisions of Clauses 17.3 to 17.7 (Key Personnel) shall apply in relation to such person.	
	1.6	The Contractor Account Security Manager shall be responsible, in consultation with the Authority Security Officer for:	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.3

		(a) the implementation of all security arrangements concerning the Contractor Personnel, the area in which they are employed, their offices and their equipment; and (b) the training and supervision of the Contractor Personnel; and shall ensure that the Contractor personnel; and procure that the Sub-Contractors comply with the security requirements set out in this Agreement.	
	1.7	Both Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing and managing security.	
	1.8	The Contractor shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Authority Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Authority Data when being used or handled by the Contractor (or their agents or sub-contractors) in performing the Services remains under the effective control of the Contractor at all times.	
	1.9	The Contractor shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document within 5 Working Days to the Authority.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.3
	1.10	The Authority and the Contractor acknowledge that information security risks are shared between the Parties and that a compromise of either the Contractor or the Authority's security provisions represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties.	
ACCREDITATION	2.1	The following Contractor solution elements shall all be accredited by the Accreditor prior to Operational Service Commencement Date: (a) commercial grade encryption for remote management of data centre equipment / data; (b) Assured LAN Interconnect (ALI) bandwidth / IP-Sec encryption for connectivity (FIPS 6.2) to Contractor premises; and (c) remote protective monitoring from the Contractor's Security Operating Centre.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.7
	2.2	To support the achievement and ongoing maintenance of accreditation of the Contractor solution elements (as set out in Paragraph 2.1), the Contractor shall:	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security

		(a) within 90 Working Days from the Effective Date, deliver an accreditation plan (the format and contents of which are to be agreed with the Authority). Such accreditation plan is to provide details of how the Contractor can achieve and maintain accreditation of such Contractor solution elements and the relevant approvals and/or associated accreditations to be obtained and maintained; and (b) prior to each Security Working Group (SWG) or as reasonably directed by the Authority, update the accreditation plan and presented it to the accreditor and the Authority (SO1 Sy) at each Security Working Group (SWG); and (c) ensure that such accreditation plan: (i) satisfies the DAIS Accreditor that all systems will provide an overall level of protection commensurate with the BIA (detailed in the 'Security and Personal Data Aspects Letter') and risk appetite; and (ii) reflects the current status of the IT Environment and accommodates all planned future Transformation, and is to be reviewed and updated once a month.	Management Paragraph: 9.5.8, 9.6.47
	2.3	The Contractor acknowledges and agrees that it bears the risk of the Contractor solution elements identified in Paragraph 2.1 being accredited by the Accreditor and that the Contractor shall be responsible for all costs associated with any remedial work required in order to achieve such accreditation.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.10
ISMS	3.1	By the date specified in the Transition Plan the Contractor shall develop and submit to the Authority for the Authority's approval in accordance with Paragraph 3.6 an ISMS (information security management system) for the purposes of this Agreement, which: (a) shall have been tested in accordance with Schedule 6.2 (Testing Procedures); and (b) shall comply with the requirements of Paragraphs 3.3 to 3.5.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.11 - 9.5.13
	3.2	The Contractor acknowledges that the Authority places great emphasis on the reliability of the Services and confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that it shall be responsible for the effective performance of the ISMS.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.11 - 9.5.13
	3.3	The ISMS shall:	Schedule 4.1 - Security Section: 9.5 Compliance Approach

		(a) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including (to the extent falling under the control and responsibility of the Contractor) the Authority Premises, the Sites, the Contractor System, the Authority System and any IT, information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Contractor in connection with this Agreement; (b) meet the relevant standards in ISO/IEC 27001 and ISO/IEC 27002 in accordance with Paragraph 7; and (c) at all times provide a level of security which: (iii) is in accordance with Law and this Agreement; (iv) as a minimum demonstrates Good Industry Practice; (v) complies with the Baseline Security Requirements contained in Appendix 1 (Baseline Security Requirements); (vi) addresses issues of incompatibility with the Contractor's own organisational security policies; (vii) meets any specific security threats of immediate relevance to the Services and/or Authority Data; (viii) minimises the impact of any security incident relating to the Authority Premises and data (including Authority Data); (ix) complies with: (A) the security requirements as set out in this Schedule; and (B) the security requirements as set out in Schedule 2.3 (Standards); (x) is in accordance with the Security Policy Framework provided that the consequences of any update to such Security Policy Framework including any additional costs are agreed by the Parties under the Change Control Procedure. (xi) is appropriate to maintain the following at acceptable risk levels (defined by the Authority in the Security and Personal Data Aspects Letter (as amended from time to time in accordance with Paragraph 4.1 of Appendix 1) in respect of: (A) loss of integrity of Authority Data; (B) loss of confidentiality of Authority Data; (C) unauthorised access to, use of, or interference with Authority Data by any person or organisation;	to Schedule 2.4 Security Management Paragraph: 9.5.11 - 9.5.13

		(D) unauthorised access to network elements (in respect of those elements of the network that are under the control of the Contractor), buildings, the Authority Premises and tools used by the Contractor in the provision of the Services; (E) use of the applications or services within the control and responsibility of the Contractor by any third party in order to gain unauthorised access to any computer resource or Authority Data; and (F) loss of availability of Authority Data due to any failure or compromise of the Services; (d) documents the security incident management processes and incident response plans; (e) document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Contractor becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Authority approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and (f) be certified by (or by a person with the direct delegated authority of) a Contractor's main board representative, being the Chief Security Officer, Chief Information Officer, Chief Technical Officer or Chief Financial Officer (or equivalent as agreed in writing by the Authority in advance of issue of the relevant Security Management Plan).	
	3.4	Subject to Clause 25.11 (Authority Data and Security Requirements) the references to standards, guidance and policies set out in Paragraph 3.3 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Contractor from time to time.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.11 - 9.5.13
	3.5	In the event that the Contractor becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3, the Contractor shall immediately notify the Authority Representative of such inconsistency and the Authority Representative shall, as soon as practicable, notify the Contractor which provision the Contractor shall comply with.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.11 - 9.5.13
	3.6	If the ISMS submitted to the Authority pursuant to Paragraph 3.1 is approved by the Authority, it shall be adopted by the Contractor	Schedule 4.1 - Security Section: 9.5 Compliance Approach

		immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Authority, the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 2 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.3 to 3.5 shall be deemed to be reasonable.	to Schedule 2.4 Security Management Paragraph: 9.5.11, 9.5.13, 9.5.15
	3.7	Approval by the Authority of the ISMS pursuant to Paragraph 3.6 or of any change to the ISMS shall not relieve the Contractor of its obligations under this Schedule.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.11, 9.5.13
SECURITY MANAGEMENT PLAN	4.1	Within 60 Working Days after the Effective Date, the Contractor shall prepare and submit to the Authority for approval in accordance with Paragraph 4.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.16 - 9.5.17
	4.2	The Security Management Plan shall: (a) be based on the initial Security Management Plan set out in Appendix 2; (b) comply with the Baseline Security Requirements; (c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Contractor; (d) detail the process for managing any security risks from Sub-contractors and third parties authorised by the Authority with access to the Services, and, to extent that the following are under the control of the Contractor (or their agents or sub-contractors), processes associated with the delivery of the Services, the Authority Premises, the Sites, the Contractor System, the Authority System and any IT, Information and data (including the Authority	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.16 - 9.5.17

		Confidential Information and the Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; (e) unless otherwise specified by the Authority in writing, be developed to protect all aspects of the Services, to extent that the following are under the control of the Contractor (or their agents or sub-contractors), and all processes associated with the delivery of the Services, including the Authority Premises, the Sites, the Contractor System, the Authority System and any IT, Information and data (including the Authority Confidential Information and the Authority Data) to the extent used by the Authority or the Contractor in connection with this Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services; (f) set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4); (g) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in Schedule 6.1 (Transition and Transformation Plans) for the Contractor to meet the full obligations of the security requirements set out in this Schedule; (h) set out the scope of the Authority System that is under the control of the Contractor; (i) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; (j) be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Authority engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule; and (k) be in accordance with the Security Policy Framework.	

	4.3	If the Security Management Plan submitted to the Authority pursuant to Paragraph 4.1 is approved by the Authority, it shall be adopted by the Contractor immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Authority, the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Authority pursuant to this Paragraph 4.3 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.16 - 9.5.18
	4.4	Approval by the Authority of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Contractor of its obligations under this Schedule.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.16 - 9.5.18
AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN	5.1	The ISMS and Security Management Plan shall be fully reviewed and updated by the Contractor at least annually to reflect: (a) emerging changes in Good Industry Practice; (b) any change or proposed change to the IT Environment, the Services and/or associated processes; (c) any new perceived or changed security threats; and (d) any reasonable change in requirement requested by the Authority.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.19
	5.2	Subject to paragraph 5.3 the Contractor shall provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Authority. The results of the review shall include, without limitation: (a) suggested improvements to the effectiveness of the ISMS; (b) updates to the risk assessments;	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.19

		(c) proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and (d) suggested improvements in measuring the effectiveness of controls.	
	5.3	Subject to Paragraph 5.4, any change which the Contractor proposes to make to this Schedule 2.4 (Security Management), the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 4.1, an Authority request, a change to Schedule 2.1 (Services Description) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.19
	5.4	The Authority may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Agreement.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.19
SECURITY TESTING	6.1	The Contractor shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after significant architectural changes to the IT Environment or after any change or amendment to the ISMS, (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Contractor so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority. Subject to compliance by the Contractor with the foregoing requirements, if any Security Tests adversely affect the Contractor's ability to deliver the Services so as to meet the Target Performance Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the Security Tests.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.20
	6.2	The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security

			Management Paragraph: 9.5.20
	6.3	Without prejudice to any other right of audit or access granted to the Authority pursuant to this Agreement, the Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Contractor, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Contractor's compliance with the ISMS and the Security Management Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. If any such Authority test adversely affects the Contractor's ability to deliver the Services so as to meet the Target Performance Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the Authority test.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.20
	6.4	Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Contractor shall promptly notify the Authority of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Authority's prior written approval, the Contractor shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements or security requirements as set out in the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Authority.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.20, 9.5.23
	6.5	If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security due to a Default or Defect of the Contractor exploiting the same root cause failure, such circumstance shall constitute a material Default for the purposes of Clause 32.1(b) (Rectification Plan Process).	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.20, 9.5.25
ISMS COMPLIANCE	7.1	The Authority shall be entitled to carry out such security audits as it may reasonably deem necessary in order:	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security

		(a) to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001, the specific security requirements set out in this Schedule and the Baseline Security Requirements; (b) to review and verify the integrity, confidentiality and security of any MOD Identifiable Information; (c) to review the Contractor's and/or any Sub-contractor's compliance with its obligations under this Schedule 2.4 (Security Compliance); and (d) to review any Documentation Deliverable, including but not limited to any documents, reports and minutes which refer or relate to the Contractor Deliverables for the purposes of Paragraph 7.1.	Management Paragraph: 9.5.26
	7.2	The Authority shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Contractor and/or Sub-contractor or delay the provision of the Contractor Deliverables and supplier information received by the Authority in connection with the audit shall be treated as confidential information.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26
	7.3	The Contractor shall, and shall ensure that any Sub-contractor shall on demand provide the Authority and any relevant regulatory body, including the Contractor's NSA/DSA, (and/or their agents or representatives), together "the Auditors", with all reasonable co-operation and assistance in relation to each audit, including but not limited to: (a) all information reasonably requested by the Authority within the permitted scope of the audit; (b) reasonable access to any Sites controlled by the Contractor or any Associated Company and any Sub-contractor and to any equipment used (whether exclusively or non-exclusively) in the performance of the Agreement and, where such Sites and/or equipment are out of the control of the Contractor, shall secure sufficient rights of access for the Auditors as shall be necessary to allow audits to take place; and (c) access to any relevant staff.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26
	7.4	If, on the basis of evidence provided by such audits, it is the Authority's reasonable opinion that compliance with the principles and practices of [ISO/IEC 27001], the specific security requirements set out in this Schedule and/or the Baseline Security Requirements is not being achieved by the Contractor, then the Authority shall notify the Contractor of the same and give the Contractor a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy. If the Contractor	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26

		does not become compliant within the required time then the Authority shall have the right to obtain an independent audit against these standards in whole or in part.	
	7.5	If, as a result of any such independent audit as described in Paragraph 7.4 the Contractor is found to be non-compliant with the principles and practices of [ISO/IEC 27001], the specific security requirements set out in this Schedule and/or the Baseline Security Requirements then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26
	7.6	The Authority shall endeavour to (but is not obliged to) provide at least 15 calendar days' notice of its intention to conduct an audit.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26
	7.7	The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under this Schedule, unless the audit identifies a material breach of the terms of this Condition by the Contractor and/or Sub-contractor in which case the Contractor shall reimburse the Authority for all the Authority's reasonable costs incurred in the course of the audit.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.26
BREACH OF SECURITY	8.1	Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or attempted Breach of Security.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.28
	8.2	Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Contractor shall: (a) immediately take all reasonable steps (which shall include any action or changes reasonably required by the Authority) necessary to: (i) minimise the extent of actual or potential harm caused by any Breach of Security; (ii) remedy such Breach of Security to the extent possible and protect the integrity of the IT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.28

		(iii) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Contractor, if the mitigation adversely affects the Contractor's ability to deliver the Services so as to meet the Target Performance Levels, the Contractor shall be granted relief against any resultant under-performance for such period as the Authority, acting reasonably, may specify by written notice to the Contractor; (iv) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and (v) supply any requested data to the Authority or the Computer Emergency Response Team for UK Government ("GovCertUK") on the Authority's request within 2 Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and (b) as soon as reasonably practicable provide to the Authority full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.	
	8.3	In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Baseline Security Requirements or security requirements as set out in this Schedule or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Authority.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.28
CO-OPERATION FOR BREACH OF SECURITY INVESTIGATIONS	9.1	Upon the occurrence of any Breach of Security: (a) the Contractor shall procure that the Authority Representative and/or any other representative or adviser of the Authority shall have the right to enter any of the Contractor Locations or any property belonging to the Contractor or a Sub-Contractor and used in performing the Services in order to investigate such breach; (b) the Contractor shall use its reasonable endeavours to make its employees (and those of Sub-Contractors) identified by the Authority Representative available to be interviewed by the Authority for the purposes of the investigation;	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.29

		(c) the Contractor shall, subject to any legal restriction on their disclosure, provide all copies of documents, records or other material of any kind which may reasonably be required by the Authority for the purposes of the investigation. The Authority shall have the right to retain copies of any such material for use in connection with the investigation; and/or (d) the Authority shall have the right to audit the Contractor's and/or Sub-Contractors' compliance with the Authority's security requirements set out in this Agreement, including this Schedule 2.4 and the Security Management Plan appended to it, in accordance with Schedule 7.5 (Financial Reports and Audit Rights)).	
	9.2	The Contractor shall, and shall procure that its Sub-Contractors shall, make available, and give reasonable assistance to the Authority Representative and/or any other representative or adviser of the Authority for the purposes of Paragraph 8.1.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.29
	9.3	Nothing in Paragraph 8.1 shall affect any entitlement to make Failure Charges and/or Withholding Deductions under this Agreement during the period in which the security investigation is subsisting or thereafter.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.29
	9.4	If the Authority's audit carried out pursuant to Paragraph 9.1(d) shows that the Contractor is not complying with the provisions of the Authority's security requirements set out in this Agreement including this Schedule 2.4 and the Security Management Plan appended to it, then the Contractor shall, at its own expense, rectify such non compliance as soon as reasonably practicable.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.29
VULNERABILITIES AND CORRECTIVE ACTION	10.1	The Authority and the Contractor acknowledge that from time to time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Authority’s information.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30
	10.2	The severity of threat vulnerabilities for Contractor COTS Software and Third Party COTS Software shall be categorised by the Contractor as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30

		(a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to 'Common Vulnerability Scoring System' (CVSS) scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and (b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.	
	10.3	The Contractor shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where: (a) the Contractor can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Contractor asserts cannot be exploited within the context of a Service must be remedied by the Contractor within the above timescales if the vulnerability becomes exploitable within the context of the Service; (b) the application of a 'Critical' or 'Important' security patch adversely affects the Contractor's ability to deliver the Services in which case the Contractor shall be granted an extension to such timescales of 5 days, provided the Contractor had followed and continues to follow the security patch test plan agreed with the Authority; or (c) the Authority agrees a different maximum period after a case-by-case consultation with the Contractor under the processes defined in the ISMS.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30 - 9.5.31
	10.4	The Contractor Solution and Implementation Plan shall include provisions for major version upgrades of all Contractor COTS Software and Third Party COTS Software to be upgraded within 6 months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless: (a) where upgrading such Contractor COTS Software and Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 months of release of the latest version ; or (b) is agreed with the Authority in writing.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30

	10.5	The Contractor shall: (a) implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body; (b) ensure that the IT Environment (to the extent that the IT Environment is within the control of the Contractor) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise; (c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Term; (d) pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Contractor) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3(e) and through the processes described in Paragraph 17.12; (e) from the date specified in the Security Management Plan (and before the first Operational Service Commencement Date) provide a report to the Authority within 5 Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Contractor) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report; (f) propose interim mitigation measures to vulnerabilities in the IT Environment known to be exploitable where a security patch is not immediately available; (g) remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Contractor Solution and IT Environment); and (h) inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment and provide initial indications of possible mitigations.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30, 9.5.32
	10.6	If the Contractor is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, the Contractor shall immediately notify the Authority.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security

			Management Paragraph: 9.5.30
	10.7	A failure to comply with Paragraph 10.3 shall constitute a Notifiable Default, and the Contractor shall comply with the Rectification Plan Process.	Schedule 4.1 - Security Section: 9.5 Compliance Approach to Schedule 2.4 Security Management Paragraph: 9.5.30
APPENDIX 1: BASELINE SECURITY REQUIREMENTS HIGHER CLASSIFICATIONS	1	The Contractor shall not handle Authority information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Contractor shall seek additional specific guidance from the Authority.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.2
END USER DEVICES	2.1	When Authority data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.3
	2.2	Devices used to access or manage Authority data and services must be under the management authority of Authority or Contractor and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Contractor devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2). Where the guidance highlights shortcomings in a particular platform the Contractor may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.3
DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION	3.1	The Contractor and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime, MOD policy or a similar regime. To that end, the Contractor must be able to state to the Authority the physical locations in which data may be	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		stored, processed and managed from, and what legal and regulatory frameworks Authority information will be subject to at all times.	Baseline Security Requirements Paragraph: 9.6.4 - 9.6.6
	3.2	The Contractor shall agree any change in location of data storage, processing and administration with the Authority in advance provided that no data shall be permitted to be stored or processed outside the UK.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.4 - 9.6.6
	3.3	The Contractor shall: (a) provide the Authority with all Authority Data on demand in an agreed open format; (b) have documented processes to guarantee availability of Authority Data in the event of the Contractor ceasing to trade; (c) securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and (d) securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.4 - 9.6.6
SECURITY & PERSONAL DATA ASPECTS LETTER (S&PDAL) (APPENDIX 3)	4.1	The Contractor hereby acknowledges the provisions set out in the S&PDAL. If the Authority amends the S&PDAL and, in the opinion of the Contractor, a change to the S&PDAL results in a material increase in the cost of providing the Services, the Contractor may submit a Change Request which shall be processed in accordance with the Change Control Procedure.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.7 - 9.6.8
	4.2	The Contractor shall protect all Information relating to the aspects designated OFFICIAL-SENSITIVE as identified in the S&PDAL in Appendix 3 to the Schedule 2.4, in accordance with the official security conditions contained in the Agreement or annexed to the S&PDAL.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.7 - 9.6.8
	4.3	The Contractor shall include the requirements and obligations set out in Paragraph 4.2 in any sub-contract placed in connection with or for the purposes of the Agreement which requires disclosure of OFFICIAL-SENSITIVE Information to the subcontractor or under which any Information relating to aspects designated as OFFICIAL-SENSITIVE is created by the subcontractor. The Contractor shall also include in the sub-contract a requirement for the subcontractor to flow the requirements of this Paragraph 4.3 to its subcontractors and through all levels of the supply chain to the lowest level where any OFFICIAL-SENSITIVE Information is handled.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.7 - 9.6.8

NETWORKING	5.1	The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least 'Foundation Grade', for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.9
	5.2	The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.9
SECURITY ARCHITECTURES	6.1	The Contractor shall apply the ‘principle of least privilege’ (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Information.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.10
	6.2	When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Contractor) the Contractor shall follow Good Industry Practice and seek guidance from the ISS Design Authority being the Authority's recognised security professionals with the appropriate skills for all bespoke or complex components of the Contractor Solution.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.10
CYBER SECURITY	7.1	The Contractor acknowledges that the Authority has determined that the Security Risk Level for this Agreement is "high" (as defined in DEFSTAN 05-138) and that such Security Risk Level may be reassessed from time to time and notified by the Authority.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11
	7.2	The Contractor shall, and shall procure that its Sub-Contractors shall: (a) comply with DEFSTAN 05-138; (b) complete the Cyber Security Model ("CSM") Risk Assessment Process in accordance with the Authority’s instructions, ensuring that any change in the Security Risk Level is notified to any affected Sub-contractor, and complete a further CSM Risk Assessment or CSM Supplier Assurance Questionnaire where a change is proposed to the Contractor’s supply chain which has or	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11. 9.6.13 - 9.6.14

		may have an impact on the Security Risk Level of this Agreement or on receipt of any reasonable request by the Authority; (c) carry out the CSM Supplier Assurance Questionnaire no less than once in each year of this Agreement commencing on the first anniversary of completion of the CSM Supplier Assurance Questionnaire; (d) having regard to the state of technological development, implement and maintain all appropriate technical and organisational security measures to discharge its obligations under this Paragraph 7 in accordance with Good Industry Practice and ISS and NCSC guidelines provided always that where there is a conflict between the Contractor's obligations under Paragraph 7.2(a) above and this Paragraph 7.2(d) the Contractor shall notify the Authority in accordance with the notification provisions in DEFSTAN 05-138 as soon as it becomes aware of the conflict and the Authority shall determine which standard or measure shall take precedence; (e) comply with all Cyber Security Instructions notified to it by the Authority as soon as reasonably practicable; (f) notify the JSyCC WARP in accordance with ISN 2014/02 as amended or updated from time to time and the Contractors NSA/DSA, and in the case of a Sub-contractor also notify the Contractor, immediately in writing as soon as they know or believe that a Breach of Security has or may have taken place providing full details of the circumstances of the incident and any mitigation measures already taken or intended to be taken; (g) in coordination with its NSA/DSA, investigate any Breach of Security fully and promptly and co-operate with the Authority and its agents and representatives and its NSA/DSA to take all steps to mitigate the impact of the Breach of Security and minimise the likelihood of any further similar Breach of Security. For the avoidance of doubt, this shall include complying with any reasonable technical or organisational security measures deemed appropriate by the Contractors NSA/DSA in the circumstances and taking into account the Security Risk Level; (h) consent to the Authority recording and using information obtained in relation to the Agreement for the purposes of the Cyber Security Model whether on the Supplier Cyber Protection Service or elsewhere. For the avoidance of doubt such information shall	

		include the cyber security accreditation of the Contractor and / or Sub-contractor as appropriate; and (i) include provisions equivalent to this Paragraph 7 in all Sub-contracts imposing provisions equivalent to this Paragraph 7 (the "equivalent provisions") and, where a Sub-Contractor breaches terms implementing this Paragraph in a Sub-contract, the Contractor shall, and shall procure that its Sub-Contractors shall, in exercising their rights or remedies under the relevant Sub-contract: (i) notify the Authority of any such breach and consult with the Authority regarding any remedial or other measures which are proposed as a consequence of such breach, taking the Authority's views into consideration; and (ii) have regard to the equivalent provisions, PROVIDED ALWAYS THAT where the Contractor has notified the Authority that it or one or more if its Sub-contractors cannot comply with Paragraphs 7.2(a) to 7.2(i) above the Authority and Contractor will seek to agree a Cyber Security Implementation Plan and where the Authority has agreed a Cyber Security Implementation Plan with the Contractor, the Contractor shall, and shall procure that its Sub-contractors shall, comply with such Cyber Security Implementation Plan until implementation is agreed to have been achieved whereupon Paragraphs 7.2(a) to 7.2(i) above shall apply in full. In the event that a Cyber Security Implementation Plan cannot be agreed the Dispute Resolution Procedure shall apply.	
	7.3	Management Of Sub-Contractors (a) The Authority agrees that the Contractor shall be entitled to rely upon the self-certification by a Sub-contractor of its compliance with its obligations pursuant to Paragraph 7.2. In the event that a Sub-contractor is found to be in breach of its obligations in Paragraph 7.2, and where the Contractor has relied upon the Sub-contractor's self-certification, the Contractor shall not be held to be in breach of this paragraph. (b) Where the Contractor becomes aware that a Sub-contractor is not complying with its obligations, the Contractor shall notify the Authority and provide full details of the Sub-contractor's non-compliance as soon as reasonably practicable and shall consult with the Authority as to the appropriate course of action which may include but not be limited to the agreement of a remedial plan or termination of the Sub-contract having regard to Condition 8.2(i).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11

		(c) Having regard to the Authority's views, the Contractor shall take all reasonable measures to address any non-compliance of a Sub-contractor in accordance with the reasonable timescales required by the Authority. Where the Contractor fails to do so, this shall amount to a breach of this Condition and the provisions of 7.2 or 7.3 as appropriate shall apply. (d) The Contractor shall, and shall procure that its Sub-contractors shall, include provisions equivalent to this Condition 4 in all Sub-contracts which flow down the obligations set out in Condition 3. of this Agreement.	
	7.4	Records (a) The Contractor shall keep and maintain, and shall ensure that any Sub¬contractor shall keep and maintain, until 6 years after termination or expiry of this Agreement, or as long a period as may be agreed between the Parties, full and accurate records including but not limited to: (i) details of all MOD Identifiable Information relating to the Contractor Deliverables provided under this Agreement; and (ii) copies of all documents required to demonstrate compliance with DEFSTAN 05-138 and this Condition, including but not limited to any information used to inform the CSM Risk Assessment Process and to carry out the CSM Supplier Assurance Questionnaire, together with any certificates issued to the Contractor and/or Sub-contractor. (b) The Contractor shall, and shall ensure that any Sub-contractor shall on request provide the Authority, the Authority's representatives and/or the Contractors NSA/DSA such access to those records as may be required in connection with this Agreement.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11
	7.5	Not Used	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11
	7.6	General (a) On termination or expiry of this Agreement the provisions of this Schedule 2.4 excepting 7.2 (b) and 7.2 (c) above shall continue in force so long as the Contractor and/or and Sub-contractor holds any MOD Identifiable Information relating to this Agreement. (b) Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the Parties under this	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.11

		Condition that have accrued up to the date of termination or expiry, including but not limited to the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry. (c) (i) The Contractor agrees that the Authority has absolute discretion to determine changes to DEFSTAN 05-138 and/or the Security Risk Level. In the event that there is such a change to DEFSTAN 05¬-138 or the Security Risk Level, then either Party may seek an adjustment to the Charges for any associated increase or decrease in costs and the Contractor may request an extension of time for compliance with such revised or amended DEFSTAN 05¬-138 or Security Risk Level provided always that the Contractor shall seek to mitigate the impact on time and cost to the extent which it is reasonably practicable to do so and further provided that such costs shall not be allowed unless they are considered to be appropriate, attributable to the Agreement and reasonable in all the circumstances. (ii) Subject to 7.6(c)(i) above, where the Contractor seeks such adjustment or extension, the Authority will proceed in accordance with the Change Control Procedure or any agreed alternative change control procedure to determine the request for adjustment or extension. The Contractor must deliver a Contractor Change Proposal to the Authority within 8 weeks of the occurrence of the change in DEFSTAN 05-138 or Security Risk Level or such longer period as may be agreed by the Parties, identifying the impact of that change and accompanied by full details of the request for adjustment. For the avoidance of doubt, the Authority shall not be required to withdraw any Authority Notice of Change which may have been issued insofar as it relates to DEFSTAN 05-138 or the Security Risk Level whether or not the Contractor Change Proposal is rejected. In the event that the Contractor does not agree with the Authority's determination, then the Dispute Resolution Procedure shall apply. (d) The Contractor shall not recover any costs and/or other losses under or in connection with this Condition where such costs and/or other	

		losses are recoverable or have been recovered by the Contractor elsewhere in this Contract or otherwise. For the avoidance of doubt this shall include but not be limited to the cost of implementing any upgrades or changes to any information system or electronic communications network whether in response to a Breach of Security or otherwise, where the Contractor is able to or has recovered such sums in any other provision of this Agreement or has recovered such costs and/or losses in other contracts between the Contractor and the Authority or with other bodies.	
PERSONNEL SECURITY	8.1	Contractor Personnel shall be subject to the Staff Vetting Procedures that include, as a minimum: employment history for at least the last three years, identity, unspent criminal convictions and right to work (including nationality and immigration status).	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.4 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15
	8.2	The Contractor shall provide comprehensive training for all Contractor Personnel and Authority Personnel (as applicable) in compliance with JSP 440 and the Authority's security requirements (as set out or referred to in this Agreement and the Security Management Plan). Such training shall be provided prior to the Contractor Personnel's engagement in the provision of any Service and thereafter on a regular basis throughout the Term as may be required due to changes in such requirements. The Contractor shall ensure that all Contractor Personnel are made aware of the relevant security arrangements and regulations on a continuous basis including through the appropriate display of security notices.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15, 9.6.17
	8.3	The Contractor shall agree on a case by case basis Contractor Personnel roles which require specific government clearances (such as ‘SC’) including system administrators with privileged access to IT systems which store or process Authority Data.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15
	8.4	The Contractor shall prevent Contractor Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15 - 9.6.16

	8.5	All Contractor Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15
	8.6	Where the Contractor or Sub-Contractors grants increased IT privileges or access rights to Contractor Personnel, those Contractor Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within 1 Working Day.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15 - 9.6.16
	8.7	If and when directed by the Authority Representative, the Contractor shall provide the Authority with a signed statement from each and every Contractor Personnel that they understand that the Official Secrets Act 1911 1989 applies to them both during and after the Term and they shall adhere to its terms.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.15
IDENTITY, AUTHENTICATION AND ACCESS CONTROL	9	The Contractor shall operate an access control regime to ensure all users and administrators of the Contractor Solution are uniquely identified and authenticated when accessing or administering the Services to the standards laid down in GPG 44 and GPG 45 (or their equivalent) at level 3 or above. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the Contractor Solution they require. The Contractor shall retain an audit record of accesses.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.18
ADMISSION TO AUTHORITY PREMISES	10.1	In respect of each Contractor Personnel, not less than ten (10) Working Days, unless by prior agreement, before such person is intended to first enter into or upon any Authority Premises in order to perform the Services, the Contractor shall provide the Authority Representative with details of such Contractor Person and any other details the Authority Representative may require (including full details of birthplace and parentage) together with details of the Authority Premises to which access is required and the capacity in which such person is concerned with the provision of the Services.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19
	10.2	The Contractor Representative shall issue a photographic pass for all Contractor Personnel (pending approval from the Authority) who are security cleared to an appropriate level for the Authority Premises pursuant to Paragraph 10.1 on or before such person is intended to enter onto any Authority Premises in order to perform the Services. All such	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19

		passes shall remain the property of the Authority and shall be surrendered on demand or on termination or expiry of this Agreement.	
	10.3	The Contractor shall ensure that the Contractor personnel and procure that the Sub-Contractors take such steps as may be necessary to obtain the security passes (including the taking of photographs, which the Contractor shall be able to provide to the Authority in electronic format).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19
	10.4	A person not in possession of a pass who is required by the Contractor or any Sub-Contractor to attend the Authority Premises to provide emergency reactive services shall be allowed temporary admission to the Authority Premises provided that the Contractor shall, and where applicable shall ensure that any Sub-Contractor shall, procure that such individual is accompanied at all times whilst at or on the Authority Premises by a member of the Contractor or Sub-Contractor's staff who has been issued with a pass pursuant to Paragraph 10.2.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19
	10.5	Whilst engaged at any Authority Premises the Contractor shall, and shall Procure that any Sub-Contractor shall, procure that all Contractor Personnel and other accompanied emergency reactive workers pursuant to Paragraph 10.3 comply with the Authority's policies relating to the conduct of staff and security arrangements as the Authority shall provide the Contractor from time to time.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19
	10.6	Notwithstanding Paragraph 6.1, the Authority may refuse any person admission to any Authority Premises or require the removal of any person from any Authority Premises: (a) if such person is not in possession of a pass pursuant to Paragraph 10.2 or is not an accompanied emergency reactive worker pursuant to Paragraph 10.3; (b) if such person, in the Authority's reasonable opinion, represents a risk to themselves or property and the Authority Representative has given notice to the Contractor Representative to this effect; (c) if the Authority has reasonable grounds for considering that the presence or conduct of such person at any Authority Premises is undesirable and the Authority Representative has given notice to the Contractor Representative to this effect; (d) as part of a security investigation pursuant to Paragraph 9 and the Authority Representative has given notice to the Contractor Representative to this effect; and/or	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.19

		(e) for any other security reason, and the Authority's decision on any matter arising under this Paragraph shall be final and conclusive.	
DISCLOSURE OF PROTECTED INFORMATION	11.1	In addition to its obligations pursuant to Clause 26 (Confidentiality), the Contractor shall not, either during or after the Term, do or permit to be done anything which it knows or ought reasonably to know may result in Protected Information being: (a) without the prior consent in writing of the Authority Representative, disclosed to or acquired by a person who is a Non-UK National or who is a British subject by virtue only of a certificate of naturalisation in which his name was included; (b) disclosed to or acquired by a person in respect of whom the Authority Representative has given to the Contractor Representative a notice, which had not been cancelled, stating that the Authority requires that Protected Information shall not be disclosed to that person; (c) without the prior consent in writing of the Authority Representative, disclosed to or acquired by any person who is not a servant of the Contractor; or (d) disclosed to or acquired by a person who is a servant of the Contractor except in a case where it is necessary for the proper performance of this Agreement that that person shall have the information.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20
Access to Protected Information	11.2	In addition to its obligations pursuant to Clause 26 (Confidentiality), the Contractor shall, both during and after the Term, take all reasonable steps to ensure: (a) that no such person as is mentioned in Paragraph 11.2 shall have access to any thing or document under the control of the Contractor containing Protected Information except with the prior written consent of the Authority Representative; (b) that no visitor to any premises in which there is anything to be supplied under this Agreement or where work in pursuance of this Agreement is being carried on shall see or discuss with the Contractor or any person employed by it any Protected Information unless the visitor is authorised in writing by the Authority Representative to do so; (c) that no copies of anything supplied or to be supplied under this Agreement or of any portion of the work carried out in pursuance of this Agreement shall be taken by the Contractor except so far as may be necessary for the proper performance thereof or with the	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20

		prior written consent of the Authority Representative, and that no such copy shall, without such consent, be published or otherwise circulated; (d) that all Protected Information and every document, model, or other thing which contains or may reveal any such information is at all times strictly safeguarded, and that, except in so far as may be necessary for the proper performance of this Agreement or with the prior written consent of the Authority Representative, no copies of or extracts from any such document, model or thing shall be made or used and no designation or description which may reveal information about the nature or contents of any such document, model or thing shall be placed thereon; and (e) that if the Authority Representative gives notice to the Contractor Representative at any time requiring the delivery to the Authority of any such document, model or thing that document, model or thing (including all copies thereof or extracts therefrom) shall forthwith be delivered to the Authority who shall be deemed to be the owner thereof and accordingly entitled to retain the same.	
	11.3	The decision of the Authority on the question of whether the Contractor has taken or is taking all reasonable steps as required by the provisions of Paragraph 11.2 shall be final and conclusive.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20
Contractor Personnel and Other Persons with Access to Protected Information	11.4	If and when directed by the Authority Representative, the Contractor Representative shall furnish full particulars of all Contractor Personnel and other persons who are at any time concerned with any Protected Information.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20
	11.5	If at any time either during or after the Term it comes to the attention of the Contractor that any Contractor Personnel acting without lawful authority is seeking or has sought to obtain information concerning this Agreement or anything done or to be done in pursuance thereof, the matter shall be promptly reported by it to the Authority Representative and the report shall, in each case, be accompanied by a statement of the facts including, if possible, the name, address and occupation of that person. The Contractor shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any Contractor Personnel, that	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20

		person shall promptly report the matter to the Contractor with a statement of the facts as referenced above.	
	11.6	The Contractor shall place every person employed by it or a Sub-Contractor who in his opinion has or shall have such knowledge of any Protected Information as to appreciate its significance, under a duty to the Contractor to observe the same obligations in relation to that matter as are imposed on the Contractor by paragraphs 11.1 and 11.2. The Contractor shall, if directed by the Authority Representative, place every person who is specified in the direction or is one of a class of persons so specified, under the like duty in relation to any Protected Information which may be specified in the direction or is one of a class of Protected Information so specified, and shall at all times use his best endeavours to ensure that every person upon whom obligations are imposed by virtue of Paragraph 11.2 observes the said obligations, and the Contractor shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Authority Representative with all necessary particulars.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.20
AUDIT AND MONITORING	12.1	The Contractor shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include: (a) Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Contractor). To the extent the design of the Contractor Solution and Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers. (b) Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Contractor) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.21
	12.2	The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the IT Environment.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

			Baseline Security Requirements Paragraph: 9.6.21 - 9.6.22
	12.3	The Contractor shall retain audit records collected in compliance with this Paragraph 10 for a period of at least 6 months.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.21
USER ACCESS CONTROLS	13.1	**Access Management** For all systems and users, the Contractor shall: (a) maintain an accurate register of user profiles, such register to be aligned to Contractor Personnel and Authority Personnel (DBS Mil Pers and Vets) roles; (b) ensure that the IT Environment is administered, managed, and controlled for Contractor Personnel and Authority Personnel (DBS Mil Pers and Vets); (c) administer, approve, and grant access (within 1 hour following approval) to accounts of the IT Environment through the trusted and agreed route in accordance with vetting standards and role-based permissions with access granted on a 'need to know' basis; (d) suspend access to accounts to the IT Environment is to be suspended within 1 hour following approval of suspension through the trusted and agreed route and delete accounts which have been continuously suspended for more than 3 months; (e) provide verification report to the Authority (SO1 Sy) confirming the review of the register of user profiles has been conducted; (f) verification and audit reports of all IT applications users to be provided on a quarterly basis to the Authority or as agreed; Content / format variable in agreement with SO1 Sy (for example, accounts suspended through failure to sign SyOps); and (g) annually review and agree all forms and procedures produced in support of system access and change on request by the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23 - 9.6.24
	13.2	**Password Management** The Contractor shall manage and control passwords to IT Environment in accordance with 'CESG Information Standard 1 and 2, DBS SyOps, and DBS Mil Pers and Vets Security Policy Manual', including: (a) ensure the IT Environment systems must force the End User to change the day one password once account access is granted; and	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.25, 9.6.80, 9.6.100, 9.6.105

		(b) ensure the IT Environment system must compel the End Users to use passwords which adhere to secure standards.	
	13.3	**User Account Authorisation** The Contractor shall: (a) manage the procedures for authorisation of new Contractor and DBS Mil Pers and Vets users and administer the password access systems relating to the IT Environment and action any Authority requests within 3 Working Days (or such timescales as agreed with the Authority); (b) in respect of DEVNET, Microsoft Office desktop environments AgencyNet Production, JPA Applications Accounts TAS 001, 002 & 004, and other authority specified requested applications, require verification of authorisation and security clearance levels; and. (c) in respect of SF applications, in addition to verification and security clearance levels, require a SF training certificate prior to despatch to the trusted and agreed route for approval.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.25, 9.6.26, 9.6.80, 9.6.100, 9.6.105
	13.4	**User Account Deletion** The Contractor shall disable access to accounts to the IT Environment as follows: (a) within 1 Working Day of a Contractor or the Authority (DBS Mil Pers and Vets) user ceasing to be authorised, or as notified by the Authority (Security Team), disable such user's authorisation (except where explicitly agreed with the Authority); (b) disable access to any accounts not accessed for 1 continuous month; (c) any disabled account not used within a further 3 month period, is to be then deleted except where explicitly agreed with the Authority (SO1 Sy); and (d) provide a monthly report to the Authority (SO1 Sy) to identify the accounts which have been deleted in the previous month to which the report relates.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.27
	13.5	**Protective Monitoring solution** The Contractor shall operate a GPG13 adherent 'Protective Monitoring' service providing a GPG18 adherent forensic capability and supported by robust incident response as follows: (a) make available and monitor 'Protective Monitoring' solution across JPA and all associated applications at all times (except for any Service Downtime as agreed with the Authority);	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.1, 9.4.8 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.28, 9.6.101

		(b) make available and monitor 'Protective Monitoring' solution across JPA and all associated applications at all times (except for any Service Downtime as agreed with the Authority); (c) unless agreed with the Authority (SO1 Sy), all 'Protective Monitoring' software is to always be within one release of the current approved version (N-1) with a clear upgrade or migration path identified; (d) all Patches and Updates are to be assessed for impact on system performance and tested before being applied in accordance with Patching requirements and timescales (contained in Appendix 3 (Patching Requirements and Timescales) to Annex M to Schedule 2.1) unless otherwise agreed with the Authority; (e) the 'Protective Monitoring' solution must have a recovery point objective (RPO) of no more than 4 hours of logs lost due to DR/BC event and a recovery time objective (RTO) the same as the main JPA application (Oracle EBS); (f) where 'Protective Monitoring' solution detects a Protective Monitoring SEV 1 or 2 event that the Contractor believes may be of interest to the Authority (SO1 Sy and/or MOD JCU), automatically notify the Authority (SO1 Sy and/or MOD JCU) within 1 hour of the observed event. Log files associated with the event are to be securely transmitted to the Joint Cyber Unit (JCU) for further analysis to maintain compliance with Op Augite; (g) perform the 'Protective Monitoring' SOC service in accordance with Incident Resolution Matrix (Appendix 2 (Incident Resolution Matrix) of Annex M to Schedule 2.1); (h) operate the Protective Monitoring Service in accordance with technical specifications. Remote administration to be carried out via the RLI and from MOD, HMG or List X sites; (i) annually review logs which are on-boarded to the 'Protective Monitoring' system and, on request from the Authority, remove logs no longer required; (j) produce and delivery to the Authority a monthly report to demonstrate the log collection is aligned with GPG13 requirements; and (k) perform and, when requested by the Authority, provide evidence that the following are being performed: (i) ensure the service generates adequate audit events to support effective identification of suspicious activity;	

		(ii) analysis such events in real time to identify potential compromises or inappropriate use of your service; and (iii) where compromise or inappropriate use are confirmed, respond promptly in accordance with published response plan informing SO1 Security at the time or within 1 Working Day.	
	13.6	**Security Operation Centre** The Contractor shall provide a Security Operation Centre (SOC) managed by an independent Contractor with continuous real time monitoring and real time auditing capability including fraud detection, for all MOD Systems and Applications managed by the Contractor. The service is to be in accordance with RMADS. The SOC shall perform as a minimum the following: (a) investigate and report all anomalies to Authority (SO1 Sy) within 1 Working Days of detection; (b) upon request from the Authority (SO1 Sy) provide specified audit reports; (c) ensure dedicated DBS Mil Pers and Veterans monitoring and resultant logs/alerts are operated and managed by appropriately cleared, authorised and trained personnel; (d) operate continuous monitoring / alerting supported by a robust 'Cyber Incident Response Plan' (in the form prescribed by the Authority from time to time); and (e) be able to either implement or trigger an appropriate response to any identified incident in accordance with the 'Cyber Incident Response Policy'.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.8 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.28, 9.6.101
	13.7	**Account Security Manager** The Contractor shall appoint an Account Security Manager (ASM) to manage and co-ordinate account security activity with the Authority (SO1 Sy) which shall be a dedicated 'CESG' certified professional and is to be permanently based at Centurion (co-located with Authority Sy Staff) and ensure the account is appropriately managed and compliant with extant policies; the ASM will be the primary point of contact for all aspects of security.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.3 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.29
	13.8	**Information Asset Owner Support** For all data that the Authority's Information Asset Owners (IAO) is responsible for, the Contractor shall manage such data to perform, as a minimum, the following:	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.30, 9.6.63, 9.6.64

		(a) provide a point of contact with knowledge of the relevant information assets, who shall attend all meetings of the 'IAO Working Group'; (b) provide all requested input to quarterly returns as directed by the IAO; and (c) provide all necessary support to the IAO (including the provision of requested data and Contractor personnel to work with the IAO) in completing Data Privacy Impact Assessments, Information Asset Registers and Data Flow Control Registers as the system Manager.	
	13.9	**Security Operating Procedures (SyOps)** The Contractor shall: (a) perform the requirements under the 'Security Operating Procedures (SyOps)' and all associated practices in accordance with the Standards and Authority policies as notified to the Contractor from time to time; and (b) 3 months following the Effective Date and every year thereafter, review and update the 'Security Operating Procedures' and all associated practices. Any amendments are to be drafted using track changes (or equivalent) stating reasons for amendment. Provide and issue to the Authority (SO1 Sy) for approval prior to publication.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.7 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.31, 9.6.88
	13.10	**Security Process and Procedure Documents** The Contractor shall establish, implement, operate, monitor, maintain, review, and update (all reviews and updates to be on an enduring basis and to incorporate additional requirements as a result of changes in MOD policies or industry best practice and only following the authorisation of the Authority (SO1 SY)) the MP&V Security Process and Procedures documents (ISMS) in consultation with the Authority (SO1 Sy) and structured as per ISO 27001 requirements and to factor in any additional requirements detailed within MOD policies.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.3 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.31, 9.6.88
	13.11	**Emerging Policy** The Contractor shall: (a) monitor and implement new HMG/MOD/DBS policy and processes as required by the Authority (SO1 Sy) and provide details and recommend the scope of any new DBS process and documents; and (b) when any new security policy and/or process is issued by the Authority (SO1 Sy), identified by the Contractor (and notified to the Authority (SO1 Sy) within 5 Working Days), or otherwise notified to the Contractor by the Authority:	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.31 - 9.6.32, 9.6.88

		(i) provide a quarterly report of all new policies and/or processes issued to the Authority (SO1 Sy); and (ii) produce an impact assessment and non-costed options for the implementation for each new Security policy and/or process within 20 Working Days of identification. Such options are to include two or more methods of implementation, noting the advantages and disadvantages of each, and subsequently recommending an option for implementation.	
	13.12	**Prior Authorisation** Prior to any change to an existing system or the development of any new system (automated and manual), ensure that it has received written authorisation from the Defence Assurance & Information Security (DAIS) Accreditor (via the Authority (SO1 Sy) or their delegated representative) and ensure that all such changes comply with security policies by the following procedure: (a) completing an 'Engineering Change Request' form to document any infrastructure changes in line with JSP604 Part 2 (Vols 1&2) for new system development and changes; and (b) minor changes to systems to be requested in writing for approval by the DBS SAC/DAIS Accreditor.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.33
	13.13	**Compliance to Regulations** The Contractor shall comply with Authority security regulations and abide by any MOD or 'Other Government Department' (OGD) regulations during visits to other sites.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.34
	13.14	**Disposal and Destruction** The Contractor shall: (a) dispose of all Authority material (equipment, media, documentation) in accordance with extant MOD security regulations; (b) following such disposal, acquire and retain a disposal certificate for destruction when required under extant policy; (c) all disposals and retention of destruction certification should be in accordance with extant regulations; (d) material declared for disposal is to be stored and managed in accordance with security regulations pending destruction; (e) all material to be accounted for at the point of disposal and or destruction in accordance with current regulations; and (f) notify those who manage the asset / inventory list when an item is disposed of within 5 Working Days.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23

	13.15	**Data Protection** The Contractor shall: (a) provide data privacy in accordance with Data Protection Legislation and the 'DBS Retention and Disposal Schedule'; (b) retain original and copy documents in accordance with 'Public Record Office' guidelines provided; (c) support Information Commissioner's Office investigations and audit requests responding within given timescales; (d) support the DBS 'Subject Access Requests' (SARs) team for responses to any Data Subject Access Requests for information in line with Data Protection Legislation; (e) manage personal data records held on the IT Environment in accordance with Data Protection Legislation and the DBS Retention and Disposal Schedule; (f) delete Personal Data records from the IT Environment upon request from the Authority IAO within 1 week of receipt of request; (g) respond to Authority requests for assistance in response to audit/inspection requests by the ICO to demonstrate joint compliance with GDPR Article 28; (h) ensure that it is complying with its obligations under GDPR Articles 32 to 36 (inclusive); and (i) notify the Authority (DPO) immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.5 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.36
	13.16	**Data Retention, Archiving and Disposal** The Contractor shall: (a) securely and efficiently, hold, archive, and dispose of Data (including reference data, metadata and associated documentation) in accordance with extant legislation and applicable Law and MOD and DBS policy; (b) retain all Data in accordance with Data Protection Legislation, the 'DBS Retention Policy', and system specific documentation such as RMADS/DPIAs and, where the retention policy is deemed unclear, seek direction from the relevant Authority IAO; (c) conduct the destruction of data in accordance with DBS and MOD Policy and NCSC Guidance; (d) gain the prior written consent of the Authority (SO1 Sy) for the use of any third parties to conduct destruction of Authority Data. The Contractor acknowledge and agrees that the Authority will only consider CPNI-certified or List X companies;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.37, 9.6.55

		(e) provide confirmation to the Authority (SO1 Sy) annually on every anniversary of the Effective Date that all soft and hard copy data held has been assessed and found to be in line with the DBS retention policy and relevant archiving and destruction activity has been undertaken; (f) where there are gaps in capability to assess data within a system the Contractor must notify the Authority (SO1 Sy) in the form of a 'Risk And Issues Notice' (RAIN) for compliance and risk assessment requirements within 5 Working Days; (g) apply Digital Continuity management in respect of information assets; and (h) facilitate the transfer of information and data to MOD CIO archives.	
	13.17	**Risk Management Accreditation Documents Sets (RMADS)** The Contractor shall develop and maintain 'Risk Management Accreditation Document Sets' (RMADS) for the IT Environment as follows: (a) develop the RMADS for the IT Environment for approval by the SAC/DAIS Accreditor; (b) on each anniversary of the Effective Date, conduct an annual review of IS1 / IS2 risk management components of the RMADS; (c) update the RMADS as directed by the Authority (SO1 Sy); (d) inform the Authority (SO1 Sy) when changes to the RMADS are required if the Authority is unaware; (e) initiate update to the RMADS upon receipt of change to threat notification; and (f) provide information to the Authority (SO1 Sy) on risk identification and management for all changes and new projects in a Security Aspects Document (SADs). SADs are to be reviewed when the associated system changes.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.7 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.38
	13.18	**Acceptance of Responsibility** The Contractor shall: (a) record and retain new starters signed acceptance of the 'Acceptable Use Policy' (AUP), SyOps, Data Protection Legislation, Official Secrets Act (OSA), the 'Breach Management, Confidentiality Agreement' and the 'New Starters Declarations' for all Contractor staff; (b) ensure that signed acceptance is obtained prior to granting an End User authority to access any data or the IT Environment; and	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.39

		(c) provide confirmation at the Authority (SWG) that the requirement is being met.	
	13.19	**IT Security Health Checks** The Contractor shall: (a) participate in DBS lead 'IT Security Health Checks' (ITSHCs) for the IT Environment (which shall not include MODNET, DWP DOI, or any applications hosted by these networks) which shall include test facilitation and the tracking, reporting, monitoring, remedial action through to completion; (b) identify and manage risks with SAC/DAIS Accreditor; (c) manage remediation through the development and maintenance of the 'Remediation Actions Register' (RAR); (d) agree with the Authority (SO1 Sy) the ITSHC plan within 10 Working Days of the Effective Date and annually thereafter; (e) provide output reports following ITSHCs within 10 Working Days of completion of ITSHC to Authority (SO1 Sy); (f) remediate all risks identified during ITSHCs in coordination with SAC/DAIS Accreditor in accordance with the DBS Risk Management Framework; (g) contribute to the DBS 'Master Remediation Actions Register' (MRAR) on request of the Authority; (h) provide a managed service of 'Security Health Checks' (ITSHCs) of the IT Environment in accordance with the Authority's requirements; (i) provide an annual penetration test for all contracted DBS infrastructure, systems and applications. This is to be done through an agreed rolling programme, produced by the Contractor and agreed by Authority (SO1 Sy); (j) perform all required remediation within 3 months of issue of the penetration report unless otherwise agreed by Authority (SO1 Sy); (k) advise the Authority (SO1 Sy) of any instance when the use of a system (manual or automated) is found to be in breach of the prescriptions of the systems accreditation within 1 Working Day; and (l) ensure the ITSHC is conducted by an independent, NCSC approved Contractor utilising security cleared personnel conforming to nationality caveats, unless otherwise agreed by the Authority.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.40
	13.20	**Right of Access**	Schedule 4.1 - Security Section: 9.6 Compliance Approach

		Within 2 working hours of request, the Contractor shall allow the Authority (SO1 Sy) unhindered access to test, inspect, analyse and audit the security functionality of the systems, and make audit trail data available to the Authority.	to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.41
	13.21	**Protective Security Audit** The Contractor shall: (a) develop an annual cycle of protective security audits in coordination with the Authority (SO1 Sy); (b) manage and update on an annual basis the 'Protective Sy Audit Cycle' documentation and provide the Authority (SO1 Sy) with the updated annual audit report each October detailing the audit findings, areas of concern and mitigation measures for consideration; (c) advise the Authority's (SO1 Sy) of any instance of Security concern or vulnerability within 1 Working Day of the occurrence; and (d) present summary reporting of activity and findings at the 'Security Working Group' (SWG)	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.41
	13.22	**Patch Management – Security Aspects** The Contractor shall: (a) monitor and report on Updates to Patches (where practicable) in accordance with the 'Patch Management Policy'; (b) report on any Updates (excluding any regular updates) to the Anti-Virus Software across all IT systems; (c) apply all Patches (to be sourced from DOBUS in the first instance and, if not available, from the vendor's website) in accordance with the Patching requirements and timescales (Appendix 3 (Patching Requirements and Timescales) of Annex M to Schedule 2.1) subject to testing; (d) monitor the deployment status for Patches and Updates to the Anti-Virus Software for all networked and non-networked CIS in accordance with Appendix 3 (Patching Requirements and Timescales) to Annex M to Schedule 2.1; (e) support Sy Governance meetings (SWG and 'Assurance Strategy' meeting) by providing updates upon request detailing: (i) Update status for AV deployed; (ii) Patch deployment status; and (iii) Patch history;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.42

		(f) review and manage all MODCERTS and report on the deployment of Patches to address the documented vulnerabilities identified to the Authority (SO1Sy); and (g) notify the Authority (SO1 Sy) where Patches cannot be deployed within indicated timelines.	
	13.23	**Security Awareness and Oversight** The Contractor shall: (a) maintain Security awareness and oversight of Contractor supplied systems and infrastructure notifying the Authority of any perceived security weaknesses, potential or otherwise and request written temporary approval to operate a system until such time as the deficiency is corrected; (b) notify the Authority in writing immediately upon discovery of a perceived security weakness; and (c) report all Security breaches in accordance with timelines detailed within JSP 541.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.43
	13.24	**Minimising Effects of a Malicious Attack** The Contractor shall: (a) minimise cross-infection following discovery of a malicious attack; (b) perform immediate action to be in accordance with the 'Cyber Incident Response Plan' and the Authority (SO1 Sy) to be informed at the earliest opportunity; and (c) follow procedures agreed with the Authority (SO1 Sy) for reporting and handling malicious content to take all reasonable measures to and assist in the formulation of a recovery plan.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.44, 9.6.107
	13.25	**CANNEL Alert State** The Contractor shall: (a) ensure the correct 'CANNEL' state (being the MOD CIS Alert State) is applied against IT Environment; (b) initiate all measures of the CANNEL alert state upon notification of change; (c) produce, by the Operational Service Commencement Date, and maintain a 'CANNEL Alert Change Response Plan' in the form as directed by the Authority (SO1 Sy). This is to be kept up to date and agreed with the Authority (SO1 Sy); and (d) monitor the CANNEL alert state, any changes are to be proactively implemented in accordance with the measures notified by the Authority, with an appropriate escalating or de-escalating response.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.45, 9.6.107

		Changes are to be notified to the Authority (SO1 Sy) within 1 Working Day of any change to the CANNEL alert state.	
	13.26	**Privileged User Access Control** The Contractor shall: (a) capture and maintain a record of Privileged Users; (b) obtain signatures from End User with Privileged Users prior to them accessing the IT Environment (and each year thereafter) to confirm their acceptance of the 'Privileged Users SyOps'; (c) provide to the Authority (SO1 Sy) a quarterly report within 10 Working Days of the end of the relevant quarter detailing the numbers of Privileged Users and confirming the access requirement; and (d) carry out a quarterly audit of Privileged Users to confirm an ongoing access requirement.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.26, 9.6.68, 9.6.80, 9.6.100, 9.6.105
	13.27	**Secure Design** The Contractor shall: (a) design and maintain a security architecture that fully satisfies the DAIS Accreditor and fully supports confidentiality, integrity and availability in accordance with the Business Impact Assessment (BIA) and Data Protection Legislation. (b) ensure all systems provide an overall level of protection commensurate with the BIA (detailed in the Security & Personal Data Aspects Letter (S&PDAL) and risk appetite.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.46
	13.28	**Public Key Infrastructure (PKI)/Defence Public Key Infrastructure** The Contractor shall: (a) Implement and manage a Public Key Infrastructure (PKI) that utilises Certification (CA) or Registration Authority (RA) certificates across all Infrastructure, applications and networks managed under this agreement in accordance with the MOD requirements unless agreed by the Authority (SO1 Sy); (b) deploy an operational PKI infrastructure for Quester Net (for example, not including the MODNET and DOI) within a time frame to be determined by the Authority, but no later than 3 years following Operational Service Commencement Date; (c) implement and maintain a Public Key Infrastructure (PKI) that utilises a Certification (CA) or Registration Authority (RA) across all Infrastructure, applications and networks managed under this agreement in accordance with the MOD requirements unless agreed by the Authority (SO1 Sy);	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.48

		(d) use assured products in the correct configuration where possible and ensure that assurance is maintained through life. Any deviations to assured products must be approved by the Authority (SO1 Sy); (e) an upstream Certificate/Registration Authority (CA/RA) must be approved by the Authority (SO1 Sy); (f) replace all existing 'Self Signed Certificates' used across the DBS estate (being digital certificates internally created and automatically authorised) with certificates issued by a Defence Public Key Infrastructure (DPKI) Certification service; and (g) extend the use of certificates across the DBS estate in accordance with requirements JSP604 (Leaflet 3005) and JSP40 (Leaflet 12).	
	13.29	**Encryption** The Contractor shall provide, deliver, maintain and upgrade encryption protection on all Authority systems and applications (insofar as technically possible).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.49, 9.6.82
	13.30	**JCU Log File Transmission** The Contractor shall: (a) securely transmit log files to JCU during supported hours in accordance with the Non-Functional Requirements & Service Availability (Appendix 1 of Annex M to Schedule 2.1), except for any Service Downtime as agreed with the Authority (SO1 Sy); (b) forward the log files to JCU in Common Event Format (CEF) on request; and (c) perform Incident Resolution to be in accordance with the Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23
	13.31	**Vulnerability Scanning** The Contractor shall: (a) provide, deliver, maintain and support a vulnerability scanning solution for the IT Environment; (b) conduct a vulnerability scan of the IT Environment once a week; and (c) send raw data scan results via an encrypted tunnel once per week to JCU.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.50, 9.6.70, 9.6.78, 9.6.82
	13.32	**Intrusion Detection and Prevention**	Schedule 4.1 - Security Section: 9.6 Compliance Approach

		The Contractor shall maintain a SNORT-compliant intrusion detection and prevention system (IDS/IPS) solution to protect the IT Environment as follows: (a) such IDS/IPS solution to be in accordance with 'Option 1' of the JCU 'Sensor Wrap' requirements document v1.1 (issued on 15 June 2016); (b) fully administer rule and signature sets on the IDS/IPS solution, including applying signature updates as required by JCU and matching GovCERT SNORT signatures against traffic; (c) enable the ability to provide 'Full Packet Capture' (FPC) files when required by JCU, including ensuring the unencrypted network traffic will be tapped via 'Switch' port mirroring via FPC; (d) ensure that the Service Levels for the SNORT-compliant IDS are in accordance with the NFR Matrix (Appendix 1 of Annex M to Schedule 2.1); (e) maintain the capability to forward IDS/IPS alerts in real time to JCU over an encrypted channel via Arcsight Enterprise Security Module (ESM); (f) apply the following signatures: (i) Government-certified SNORT signatures when made available; (ii) Intelligent-based signatures to be applied as supplied and required by JCU; and (iii) DPKI certificates to be used on the IT Environment; (g) forward the log files to JCU in Common Event Format (CEF) on request; (h) apply all Patches for the transmission of the log files in accordance with Patching requirements and timescales (Appendix 3 of Annex M to Schedule 2.1); and (i) perform Incident Resolution to be in accordance with the Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1).	to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.51, 9.6.76
	13.33	**Information Assurance Maturity Model (IAMM)** The Contractor shall: (a) ensure Information Assurance Maturity Model (IAMM) Levels 1, 2 and 3 are delivered and maintained at all services applicable under the contract; (b) provide responses to Authority IAMM audit requests / returns within 5 Working Days;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.52

		(c) generate and maintain the IAMM compliance plan that is approved by the Authority (SO1 Sy); and (d) conduct a gap analysis of IAMM levels 1, 2 and 3 within 6 months of Effective Date and annually thereafter and provide the results to the Authority within 5 Working Days of completion, including a plan to achieve compliance.	
	13.34	**Data Flow Control** The Contractor shall: (a) report all data exchanges managed by the Contractor to the Data Flow Control Register (DFCR) Manager. Proactively review data exchange methods to ensure secure and pragmatic practices are applied; (b) support the Authority in its annual audit of the DFCR; (c) inform the DFCR Manager of new or changes to existing data flows prior to transmission; (d) coordinate with the Authority to ensure mandated data sharing agreements are in place prior to data sharing commencing; (e) inform the DFCR manager when a data flow ceases within 5 Working Days; (f) complete annual returns for the DFCR verification process as requested by the DFCR Manager within 2 weeks of the request from the DFCR Manager; and (g) identify any irregularities with a data exchange and report to the Authority within 1 Working Day of discovery of the irregularity.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.53
	13.35	**Data Protection Impact Assessments** The Contractor shall: (a) provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment (DPIA) (an assessment by the Authority of the impact of the envisaged processing on the protection of Personal Data) prior to commencing any processing; (b) provide responses to the Authority's requests for DPIA assistance within 5 Working Days and such responses to include: (i) a systematic description of the envisaged processing operations and the purpose of the processing; (ii) an assessment of the necessity and proportionality of the processing operations in relation to the Services; (iii) an assessment of the risks to the rights and freedoms of Data Subjects; and	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.54

		(iv) detail the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.	
	13.36	**Data Storage** The Contractor shall: (a) ensure that all information for which DBS MP&V is the custodian and held or processed by the Contractor is marked, stored, afforded protection and disposed of in accordance with current regulations and in accordance with the regulations on aggregation of bulk data; and (b) conduct an annual protective security audit for all systems and locations and report to the Authority (SO1 Sy) in the SWG following completion of the audit.	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.55
	13.37	**Remote Working** The Contractor shall: (a) ensure that all Contractor Personnel and personnel of any Sub-Contractor (and their sub-contractors) who are delivering services to the Authority from a non-MOD location (including at the Data Centres or home working) provide annual assurance that JSP 440 and other applicable standards are being fully adhered to in line with the 'Security Aspects Letter' provided by the Authority (b) produce an 'Annual Security Assurance Report' on an annual basis to be delivered to the Authority (SO1 Sy) by the end of August during the relevant year. Such report to be in the format and with the content as required by the Authority (SO1 Sy) (as notified to the Contractor from time to time) and include, but not be limited to, a confirmation that the Contractor is compliant with the 'Classified Materials Assessment Tool' (CMAT).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.55
	13.38	**Key & Combination Control** The Contractor shall: (a) maintain all Contractor managed keys and combinations in accordance with current regulatory requirements; (b) report to the Authority on an annual basis on all Contractor managed keys and combinations in accordance with the JSP 440. This report is to be provided to the Authority within 1 week of completion and routinely reported to the Authority (SO1 Sy) at the SWG; and (c) all discrepancies are to be reported to the Authority (SO1 Sy) within 2 Working Days.	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.57

	13.39	**Authorised Access Lists** The Contractor shall: (a) maintain access lists for Data Centres, 'Branch Offices' and Communications rooms to ensure only authorised personnel are permitted access; (b) lists to be reviewed and re-verified monthly; and (c) access lists to be updated immediately of notification of the user's authorisation being rescinded.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.57
	13.40	**Identity/Warrant Card Production – Security Aspects** The Contractor shall: (a) securely issue, deliver identity documents and maintain auditable accounting for all blank, yet to be issued, DMASC, MOD F90, and 'Warrant Cards' held awaiting issue within DBS; (b) maintain auditable records of secure storage and issue of identity documents; (c) all discrepancies identified in the audit are to be reported to the Authority (SO1 Sy) immediately; (d) all discrepancies identified in the audit are to be duly investigated by the Contractor and a report is to be submitted to the Authority (SO1 Sy); (e) conduct a quarterly muster of all blank cards and report the findings to the Authority (SO1 Sy) within 5 Working Days of the completion; (f) account for all blank DMASC, MOD F90 and Warrant Cards held within DBS (e.g. the blanks held on account, prior to production) and those DMASC MOD F90 and post production Warrant Cards stored at DBS prior to issuing to the Units; and (g) storage and accounting procedures to be agreed with the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.57
	13.41	**Physical Security** The Contractor shall: (a) provide and maintain a secure physical environment at all Contractor managed locations utilised for the delivery of DBS Services; (b) provide access controls and physical security procedures at all locations utilised for the delivery of DBS Services; (c) produce a programme of Annual Audits of the physical controls at Contractor managed sites. The audit report is to be delivered to the SO1 Sy within 1 week of completion; and	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.10 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.57

		(d) all procedures and controls are to be agreed by the relevant Authority SME prior to implementation.	
	13.42	The Contractor shall: (a) ensure authorised visitors are allowed access to Contractor managed buildings and maintain visitor access lists for all Contractor managed buildings; and (b) reconcile any issued passes on a daily basis and to investigate and report any discrepancies within 1 Working Day to the Authority (SO1 Sy) at all times.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.23, 9.6.57
RISK MANAGEMENT	14.1	**Risk Management Framework** The Contractor shall comply with and contribute to the 'DBS Risk Management Framework' as follows: (a) from the Effective Date, establish and fully implement a security risk management framework in accordance with the 'DBS Risk Management Framework'; (b) demonstrate conformance with a recognised standard which includes controls which articulate how well a governance framework manages a particular service; and (c) maintain a documented framework for security governance, with policies governing key aspects of information security relevant to the service. Documentation is to be reviewed and agreed with the Authority (SO1 Sy) annually and is to compliment DBS Policy.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.58 - 9.6.59
	14.2	**Risk Identification and Recording** The Contractor shall: (a) maintain risk registers for contracted systems and applications and SME input to the 'DBS Risk Management Process'; (b) upon confirmation of a potential risk identified by the Contractor, a 'Risk And Information Notice' (RAIN) is to be raised and submitted to Authority (SO1 Sy); (c) provide a suitable subject matter expert for attendance on an as required basis at all 'Security Risk Balance Case' meetings; and (d) compile appropriately detailed RBCs, RAINs and remediation plans for all potential risks identified. Documents produced are to identify all potential courses of action, together with their associated advantages and disadvantages.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.58 - 9.6.59
	14.3	**Accounting for Information Bearing Assets** The Contractor shall:	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		(a) account for information bearing assets (including hardware and software applications) for DBS throughout their life; (b) conduct an annual review (every January) of the procurement, storage, distribution and decommission process for Information bearing Assets reporting the findings to the Authority (SO1 Sy) within 10 Working Days of completion; (c) produce and maintain an auditable 'Information Bearing Asset Register' detailing all Hardware with sufficient information to enable the Authority to identify and track the Hardware (which shall include as a minimum the make, model, serial number, storage capacity (if applicable)); (d) monitor the distribution and use of all 'Removable Media' (RM) on a quarterly basis (Jan, Apr, Jul, Oct); (e) provide an annual report detailing the distribution and use of all 'Removable Media' (RM) report to be delivered to Authority (SO1 Sy) in Oct each year; (f) conduct annual inventory check of all laptops. Report to be delivered to Authority (SO1 Sy) by Jul each year; and (g) provide a report to the Authority within 10 Working Days of completion of every census, or inventory check.	Baseline Security Requirements Paragraph: 9.6.60, 9.6.78, 9.6.97, 9.6.98
	14.4	**Security Point of Contact** The Contractor shall: (a) provide a security point of contact to respond to DBS users and customers in regard to security related queries and requests for information; and (b) respond within 2 Working Days, to the following: (i) 'First Resolving Group' to check and respond to reports that are provided via the Centre for the Protection of the National Infrastructure (CPNI) website reports); (ii) 'First Resolving Group' to check and respond to MOD CERTs); and (iii) Security Incidents reported to the Help Desk or the Contractor's Security staff.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.61, 9.6.68, 9.6.80, 9.6.100, 9.6.105
	14.5	**Security Incident Reporting** The Contractor shall: (a) provide to the Authority details of all security events across all DBS sites via submission into the 'DBS Security Incident Log'; (b) report all security breaches, security near misses, security incidents and security weaknesses identified to the Authority (SO1	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.62

		Sy) within 1 Working Day. Reporting format is to be in accordance with the JSP 541; (c) update the 'DBS Security Incident Log' accordingly within 1 Working Day; (d) information arising from the investigation of security occurrences and incidents shall be protected and handled on a need-to-know basis, and documentation of these matters given a suitable protective marking on a case by case basis; and (e) investigation reports ('Initial', 'Interim', and 'Final') to be provided to the Authority for submission into the Incident Log within the following timescales (Initial: 1 Working Day of notification of the occurrence / Interim: As agreed with the Authority (SO1 Sy), Final: within 5 Working Days of completion of the investigation).	
	14.6	**Security Incident Reporting** The Contractor shall: (a) proactively, or as directed by the Authority (SO1 Sy) investigate all security breaches, security incidents, security weaknesses, potential incidents, or other event/occurrence; (b) investigations to be completed in a proactive and timely manner and reported within the timescales at Paragraph 14.11; (c) Investigation reports and updates are to contain sufficient information for the completion of the 'MISIRS submission form'; and (d) submit all reports to the Authority (Integrated Security Assurance Team and SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.62
	14.7	**Security Incident Mitigation** The Contractor shall: (a) propose and implement actions agreed with the Authority (SO1 Sy) to mitigate the impact of any security incident with a view to preventing a reoccurrence; and (b) in response to a notified security incident, review initial information reported and propose measures to mitigate the impact of or prevent further instances of the event in question with measures adopted to be agreed with the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.62
	14.8	**Security Vetting** The Contractor shall: (a) ensure all Sub-Contractors (and their sub-contractors) hold required security clearance as detailed within this Schedule;	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.6 Section: 9.6 Compliance Approach

		(b) ensure compliance with the vetting requirements and facilitate the provision of all information required to support the vetting process (initial or through life). Such security vetting and development vetting requirements are detailed within 'Schedule 2.4/S&PDAL' (as reviewed and amended by the Authority (SO1 Sy) from time to time). Developmental vetting is required for all Privileged Users and those security positions as identified by the Authority; (c) maintain a database of all vetting clearances for Sub-Contractors ensuring vetting renewal actions are always completed prior to expiry; (d) carry out security briefs and debriefs in accordance with extant regulations; (e) notify the Authority (SO1 Sy) of any Sub-Contractor not holding the required vetting status prior to any engagement or commencement of employment at any DBS site. Appropriate RBC SREs to be submitted to Authority (SO1 Sy) no later than one week prior to commencing employment in all instances; and (f) on a monthly basis produce a list, categorised by each DBS site, of those Sub-Contractor and third party personnel working at risk with the prior approval of the Authority (SO1 Sy) and provide a copy to the Authority (SO1 Sy).	to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.63, 9.6.64
	14.9	**Suitability to Hold Security Clearance** The Contractor shall: (a) inform the Authority (SO1 Sy) of any information which becomes available to the Contractor which may suggest that any of the Contractor Personnel may no longer be suitable for such work, even though security clearance may have previously been granted. Within 1 Working Day of such discovery, the Contractor shall raise and submit 'Aftercare Incident Reports' (AIR) in accordance with JSP440 and inform the Authority (SO1 Sy); (b) where a Security Incident gives rise to an AIR, then confirmation that the AIR has been sent is always to be provided within the final report; and (c) list the number of AIRs submitted in Annual Security Assurance Report.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.65
	14.10	**Security Education & Awareness** The Contractor shall: (a) provide initial, annual and ad-hoc security education to ensure all Contractor Personnel engaged in the provision of Authority	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		services are aware of their security responsibilities and have undergone adequate training in the use, care, protection and handling of Personal Data; (b) obtain annual assurance from Sub-Contractors and third parties that their employees are aware of their security responsibilities, and that assurance must be made available to the authority; (c) provide annual assurance that Sub-Contractors receiving and processing authority data are aware of their security responsibilities which as flowed down through a 'Security and Personal Data Aspects Letter'; (d) develop and maintain and deliver annual security and information assurance briefs and deliver annually to all DBS Contractor employees; (e) develop and deliver themed security awareness campaigns (posters, entries in DBS publications, all user messages). No more than 12 awareness campaigns per annum; and (f) ensure Contractor staff complete periodic mandatory training as identified by the Authority (SO1 Sy).	Baseline Security Requirements Paragraph: 9.6.64
	14.11	**Freedom to Investigate** The Contractor shall: (a) allow any investigative body authorised by the Authority (SO1 Sy) free access to Contractor sites, records, information and staff deemed relevant to the investigation of any security occurrence; and (b) upon request from the Authority (SO1 Sy) grant the nominated investigative body authorised by the Authority (SO1 Sy) free access to Contractor sites, records, information and staff deemed relevant to the investigation of any security occurrence.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.5.46, 9.6.66
	14.12	**SAC Secondment** The Contractor shall second a dedicated resource to act as the Security Assurance Coordinator (SAC) working directly for the Authority (SO1 Sy) and in close coordination with the DAIS Accreditor to provide specialist technical advice in support of the accreditation of contracted systems and applications. SAC to hold in date CESG Certified Professional Senior Information Risk Advisor certification (CCP SIRA) at all times.	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.5, 9.4.11
	14.13	**Crypto Services** The Contractor shall (a) provide 'Crypto' services, including a 'Custodian' and 'Deputy Custodian', for DBS MP&V and HMS Sultan in accordance with	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		JSP 490 and DBS MP&V Security Policy Manual. Such 'Custodian' and 'Deputy Custodian' to be suitably qualified in accordance with applicable regulations. For the avoidance of doubt, the joint arrangement with HMS Sultan is location-specific and is not applicable if the Services are no longer conducted from this location; (b) support monthly audits and annual audits conducted by the Authority (Supervising Officer); and (c) respond to 'National Crypto Authority Annual Audits'.	Baseline Security Requirements Paragraph: 9.6.67, 9.6.82
	14.14	**Privileged Access Management** The Contractor shall, in accordance with Paragraph 18.4, monitor and apply Privileged User access management controls as follows: (a) all Privileged Users system usage to be recorded and analysed in accordance with Good Practice Guide (GPG) 13 at all times; (b) monitoring information is to be retained for 7 years and made available within 5 Working Days of a formal request being submitted by the Authority (SO1 Sy); (c) audit the accounts of Privileged Users to identify irregular activity and present a report to the Authority (SO1 Sy) at the 'Security Working Group' (SWG); and (d) confirm any anomalies identified are to be reported to the Authority (SO1 Sy) within 1 Working Day and investigated immediately. An initial report is to be provided to the Authority (SO1 Sy) within 1 Working Day followed up by regular briefs on a frequency agreed by the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9
BULK DATA MEASURES	15.1	The Contractor shall fully comply with the mandated NCSC Bulk Data Measures as published and periodically reviewed, in applying the requirements contained within this Schedule.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.69
	15.2	**Understand and Actively Manage Vulnerabilities** The Contractor shall: (a) using publicly available resources and available MOD resources (for example, the 'Cyber Security Information Sharing Partnership – CiSP' and the 'Ministry of Defence Computer Emergency Response Team – MODCERT'), maintain and actively manage an awareness of unmitigated vulnerabilities that are identified within DBS MP&V Information and Communications Technology assets, ensuring that awareness can be used to address risk and identify	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.28, 9.6.70, 9.6.78, 9.6.82, 9.6.101

		mitigations that are agreed with the authority in consideration for application; (b) track, prioritise and mitigate in accordance with the regulations announced vulnerabilities for software packages, network equipment and operating systems in use in acceptable timescales agreed with the Authority (SO1 Sy); (c) utilise 'CHECK'-certified third parties, as agreed with the Authority (SO1 Sy) for testing to confirm that internal expectations are matched by test findings; (d) take all reasonable actions to ensure that known vulnerabilities in the Software and Hardware are mitigated; (e) ensure all software on externally-accessible Hardware has had all security Patches applied (or vulnerabilities otherwise mitigated) in accordance with Appendix 3 of Annex M to Schedule 2.1 (Patching Requirements and Timescales); (f) automate Patch management system across all systems and network attached devices; (g) security test all Software and Applications for common vulnerabilities prior to handling live data; (h) utilise market leading (both commercial sources and Open Source) external vulnerability intelligence services to maintain awareness of threats to the system; (i) within tolerable levels of risk, carry out procedures in line with Good Industry Practice to identify vulnerable surfaces and investigate whether they can be removed or protected in a better fashion than would normally be dictated by an OFFICIAL system (including but not limited to implementing BPDM3). Where any vulnerability is identified within COTS software, vulnerabilities should be mitigated by other means until such time as a vendor patch or update is provided; (j) provide an automated mechanism for vulnerability identification and management across the network as follows: (i) prior to the scan taking place, advise the Authority on the technical and performance impact of conducting any full/partial scans and, working with the Authority and taking advice from JCU, ensure that the principles of such advice are incorporated into that scan and all future relevant scans; and	

		(ii) as any network-wide vulnerability scan is likely to have a performance impact (which could be exacerbated by the nature of the scan and the frequency at which they are conducted), undertake scans at a point which will minimise any disruption to the Service (unless agreed otherwise with the Authority); and (iii) scans of network vulnerability are to be at the frequency agreed with the Authority to ensure that all Authority (DBS Mil Pers and Veterans); (k) enable and conduct effective vulnerability / event correlation to aid attack identification and verification of logging activities which are to be subject to continual analysis; and (l) ensure that all logs are available to the protective monitoring system 100% of the time. Make available all such logs to the protective monitoring system.	
	15.3	**Unsupported Software/Hardware** The Contractor shall: (a) ensure no unsupported software is present within the IT Environment and its underlying infrastructure; (b) ensure that all operating systems, software packages and networking equipment for components which handle or secure access to data are in support by the vendor or community; and (c) brief the Authority (SO1 Sy) through the Security Working Group (SWG), if a component upgrade falls outside N-1.	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.71, 9.6.98
	15.4	**Bulk Data Access/Export** The Contractor shall: (a) ensure that all exporters and users of bulk information are known by personal user identification, location and download pattern, and that any deviations from the known pattern are detectable and that an alert is raised where a deviation occurs; (b) establish monitoring to detect unusual queries, attempted large scale exports of data or administrator access to data; (c) from 3 months after the Effective Start, conduct quarterly tests of control measures in place and report failures to the Authority (SO1 Sy) together with mitigation measures to address the failure; (d) for End Users whose permissions allow access to more than 1,000 records, their pattern of download over time is established within the 'Protective Monitoring System' as a behavioural characteristic; and	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.72

		(e) with the download behaviour of End Users established, deviations from the pattern in excess of 10% (or such other percentage as notified by the Authority from time to time) of overall norm of download is reported to the Authority (SO1 Sy) within 1 Working Day of an event outside the known behaviour pattern being identified/confirmed.	
	15.5	**Rate Limiting** The Contractor shall: (a) rate-limited (managed, limited and controlled) End User access to bulk data is to agreed levels; and (b) ensure that End Users are only permitted to download data in accordance with their established role-based permissions.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.72
	15.6	**Retain only Necessary Data** The Contractor shall: (a) ensure that all backups or copies of Authority data managed by the contract are held securely, and retained in accordance with the 'DBS Retention & Disposal Schedule'; (b) encrypt and store all copies of data required for temporary activities (including but not limited to error checking, Application code validation, error fixing, and all such other instances as agreed with the Authority) and delete immediately when no longer required or at the request of the Authority; (c) ensure that no live data is used in test or development systems, unless these systems are protected to the same level as the production systems; and (d) ensure that all uses of live data for testing purposes are approved by the Authority (SO1 Sy) prior to execution of the tests.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.73
CESG REQUIREMENTS AND RECOMMENDATIONS	16.1	**Reduce Data Holdings** Creation, Retention and Archiving (CRAD) has been conducted utilising an individual 'whole record' approach, with the record being retained for the longest retention period identified. In this regard it is considered that JPA and its associated applications are not wholly compliant with current Data protection Legislation and NCSC Requirements. Action is required in regard to the application of MOD data retention, archiving and destruction policy at the data item level whilst not detracting from the integrity of individual records within relational databases. The Contractor shall: (a) ensure only active/necessary records are held within JPA and any supporting applications;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.74, 9.6.75

		(b) identify scope for archiving within JPA and its associated applications and identify business processes impacted by archiving; and (c) prior to archiving non-active data ensure mitigation measures are agreed with the Authority and in place.	
	16.2	**Intrusion Prevention Service** The Contractor shall configure the 'Intrusion Prevention System' (IPS) to detect current threats and the currency against emerging threats to be maintained utilising threat intelligence signatures received from the Authority (MOD Certs) within 1 calendar day of receipt as follows: (a) conduct testing on all industry security signatures (includes open source, commercial or any other viable source of security signatures) to ensure that the installation of such a signature will not trigger against a standard set of BAU traffic and, where it can be shown that a signature will trigger an interruption to BAU traffic, immediately notify the JCU; (b) immediately following completion of testing in accordance with Paragraph 16.2(a), install such industry security signatures in the IPS; (c) Oracle specific rules to be set in accordance with recommended guidance (including GPG13 and other sources at all time); (d) F5 configuration to be always validated by pen-test during initial application installation; and (e) employ 'White Listing' at all time.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.76
	16.3	**WEB Application Firewalls** The Contractor shall: (a) ensure that Web Application Firewall (WAF) protection is in place and active; (b) ensure that Layer 7 Web Application Firewall protection is active at all times; and (c) custom rules provided by, or configured with the aid of the Joint Cyber Unit or derived from commercial sources or internal intelligence are installed into the WAF after testing (if required).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.76
	16.4	**Bring Your Own Device (BYOD)** The Contractor shall: (a) where 'Bring Your Own Device' (BYOD) access is enabled with interactive functionality, follow guidance from Information Systems and Services (ISS) on deploying cross domain techniques to manage the risks;	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.7 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		(b) implement 'Cross Domain Measures' for BYOD in accordance with ISS requirements at all times; and (c) ensure that all internet-facing BYOD is secured and delivered with user 2FA and dynamic identity confirmation compliant with the standards set out in GPG44 and GPG 45 at level 3 or above.	Baseline Security Requirements Paragraph: 9.6.77
	16.5	**Cryptography** The Contractor shall: (a) maintain the configuration of the cryptography used to protect system-system interactions at all times; (b) where 'HMG Issued Cryptographic' systems or materials are used, then the requirements within JSP604, JSP490 and JSP491 are to be complied with; (c) where commercial cryptographic products (hardware or software) are used, the Contractor is to maintain awareness of any vulnerabilities in the products used to ensure that cryptographic products remain suitable at all times; and (d) where vulnerability has been identified in a commercial cryptographic product, the Contractor will do a risk analysis to identify what mitigations can be applied. All application of mitigations to be agreed with the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.78, 9.6.82
	16.6	**Minimising Required Fields** The Contractor shall actively reduce the impact of compromise by redacting, anonymising and limiting fields to the minimum required for each particular business use case.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.79, 9.6.80, 9.6.100, 9.6.105
	16.7	**Network Management Infrastructure Separation** The Contractor shall provide logically and physically separate network management infrastructure and terminals (with separate AD and supporting services) to reduce the risk of internet-borne attacks through Network access.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.80, 9.6.100, 9.6.105
	16.8	**Privileged Access Management & 2Factor Authentication** The Contractor shall utilise 'Privileged Access Management' technologies, in conjunction with 'Two-Factor Authentication', to monitor and limit Privileged User actions on a ticket-by-ticket basis.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.80, 9.6.100, 9.6.105
NCSC CLOUD SECURITY PRINCIPLES	17.1	**Data In Transit Protection** The Contractor shall:	Schedule 4.1 - Security Section: 9.6 Compliance Approach

		(a) ensure that End User data transiting networks is adequately protected against tampering and eavesdropping. The Contractor must always actively employ approved security measures to protect user data in transit; (b) not use SSL versions or TLS versions earlier than 'Version 1.2'; (c) if it is unable to utilise a recommended security measure and no alternative is available, view such lack of security measure as a risk and treated as such; (d) if an in-use 'Security Enforcing' function fails for any reason, advice is to be sought from the Authority (SO1 Sy) before any insecure transmission takes place; (e) immediately notify the Authority if a transmission occurs which is subsequently found to be insecure in order that counter-compromise measures can be implemented; (f) notify the Authority (SO1 Sy) prior to every transmission of live data where the Contractor is not able to utilise MOD recommended security measures; and (g) ensure that 'Defence Public Key Infrastructure Services' are always utilised to provide Information Security.	to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.81, 9.6.82
	17.2	**Asset Protection and Resilience – Identified Locations** The Contractor shall ensure that all physical locations used to process, storing or manage user data are known to the Contractor and the Authority (SO1 Sy). Data is only to be processed and stored at locations identified and acceptable to the Authority (SO1 Sy).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph:
	17.3	**Asset Protection and Resilience – Security Standards** The Contractor shall: (a) ensure that the physical and emissions Security of all Data Centres meets the standards acceptable to the Authority at all times and provide a monthly report of such physical and emissions security to the Authority (SO1 Sy); (b) ensure that Data Centres used are always certified to a recognised standard (which incorporates physical security). Such recognised standards include, but are not limited to, CSA CCM v3.0, SSAE-16 / ISAE 3402, and List X Standards; (c) facilitate an annual inspection and audit of the security measures implemented within the Data Centres by an independent organisation (e.g. DAIS, or a body associated with the standard applied to the Data Centre) or the Authority (SO1 Sy, or personnel nominated by SO1 Sy), and will ensure that the results of the audit	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.83

		are available to the Authority (SO1 Sy) in accordance with a timetable to be agreed with the inspecting body prior to the inspection or audit occurring; (d) ensure that 'TEMPEST' standards as identified in JSP440 are met at all times; and (e) grant the Authority (SO1 Sy), or personnel nominated by the Authority (SO1 Sy), access to Data Centres within 5 Working Days of the request at all times.	
	17.4	**Asset Protection and Resilience – Data Security** The Contractor shall: (a) protection of 'Data at Rest' is to receive a level of protection commensurate with its protective marking and in consideration of impact if compromised; (b) always employ encryption, obfuscation techniques or data storage 'sharding'; and (c) at all times employ encryption to ensure that no data is written to disk in unencrypted form.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.6 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.84
	17.5	**Asset Protection and Resilience – Data Sanitation** The Contractor shall apply 'Data Sanitisation' processes (utilising Authority or NCSC approved tools or devices) to ensure the secure destruction of data as follows: (a) provide the capability to securely delete data at the field level in accordance with the data destruction standards of the Authority and National Cyber Security Centre (NCSC); (b) ensure that any Storage media no longer required is sanitised according to a specified policy; (c) provide evidence on request from the Authority that previously stored data cannot be accessed by others after storage media is released.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.85
	17.6	**Asset Protection and Resilience – Destruction and Disposal** The Contractor shall: (a) dispose of all hardware and other information bearing equipment in accordance with the 'CPNI Destruction Standard ' commensurate with the level of information carried on the asset; (b) ensure a destruction service which specialises in secure disposal of equipment, which has been assessed against a recognised standard, is utilised; and	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.85

		(c) coordinated equipment disposal with Asset owners and appropriate records maintained in accordance with asset management process.	
	17.7	**Asset Protection and Resilience – Resilience and Availability** The Contractor shall: (a) ensure 'Physical Resilience' and 'Availability' in accordance with the requirements contained in Schedule 8.6 (Business Continuity & Disaster Recovery) and ensure that such minimum levels of service availability are specified in any service level agreement with Sub-Contractors; and (b) provide details and evidence to the Authority on request of how the Contractor has designed its solution to be resilient. The Contractor acknowledges that any support services in third party contracts not provided as a contractual obligation (for example, performed through 'reasonable endeavours') shall be deemed to have no guaranteed support for the purpose of this Paragraph 17.7.	Schedule 4.1 - Security Section: 9.4 Account Security Service Composition Paragraph: 9.4.10Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.86
	17.8	**Separation between users** When implementing a shared cloud service, the Contractor shall: (a) ensure the separation between cloud tenants; (b) provide evidenced assurance as to the integrity of separation of tenants within the cloud services prior to implementation of the shared cloud service and annually thereafter for the life of the service; and (c) carry out penetration testing of the shared cloud service to ensure the products and security controls have been configured in accordance with Good Industry Practice and that there are no common or publicly known vulnerabilities in the tested components (at the time of the test) and ensure that such penetration testers are appropriately qualified (for example, individuals certified under the 'CHECK', CREST', or 'Tiger schemes).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.87
	17.9	**Governance and Compliance** The Contractor shall: (a) abide by the DBS MP&V Security Information Assurance Risk Governance process; (b) security and information security are to be included as part of the Contractor's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risks;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.88

		(c) demonstrate conformance with a recognised standard which includes controls which articulate how well a governance framework manages a particular service at all times; (d) nominate a clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. Changes to the nominated individual are to be notified to the Authority (SO1 Sy) within 5 Working Days of being made; (e) maintain a documented framework for security governance, with policies governing key aspects of information security relevant to the service. Documentation is to be reviewed and agreed with the Authority (SO1 Sy) annually; and (f) identify and ensure compliance with applicable legal and regulatory requirements. Non-compliance should be notified to the Authority (SO1 Sy) within 5 Working Days of discovery, together with details of mitigation measures adopted.	
	17.10	**Configuration and Change Management** The Contractor shall: (a) ensure that Configuration and Change Management Procedures are implemented such that all network assets are accountable, and their configuration status is known; (b) the status, location and configuration of service components (both hardware and software) are to be continuously tracked throughout their lifetime; and (c) assess all Changes for potential security impact, then managed and tracked through to completion. The Service Contractor provides evidence of this to the Authority (SO1 Sy) through the Security led 'Assurance Strategy' meeting.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.89
	17.11	**Operational Security - Vulnerability Management** The Contractor shall: (a) deploy a network wide capability to identify vulnerabilities which have been determined and listed by known reliable (commercial and Open Source) vulnerability intelligence sources; (b) at a frequency to be agreed with the Authority (SO1 Sy), provide evidence that the following are being undertaken:	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.90

		(i) potential new threats, vulnerabilities or exploitation techniques which could affect service delivery are assessed and corrective action is taken as required; and (ii) relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored and the severity of threats and vulnerabilities is considered within the context of the business and this information is used to prioritise the implementation of mitigations; (c) track known vulnerabilities using a suitable risk management process until mitigations have been deployed and tested and demonstrate assurance conformance with a recognised standard. Any non-conformance of this Paragraph is to be notified to the Authority (SO1 Sy) within 5 Working Days; and (d) provide timescales for implementing mitigations for the Authority's approval.	
	17.12	**Operational Security - Protective Monitoring.** The Contractor shall: (a) operate a GPG13 adherent Protective Monitoring service providing a GPG18 adherent forensic capability and supported by robust incident response; (b) perform the Protective Monitoring service should be in accordance with Incident Resolution Matrix (Appendix 2 of Annex M to Schedule 2.1); (c) when requested by the Authority, provide evidence that the following are being met: (i) the service generates adequate audit events to support effective identification of suspicious activity; (ii) these events are analysed in real time (24/7) to identify potential compromises or inappropriate use of your service; and (iii) where compromise or inappropriate use are confirmed the Contractor is to respond promptly in accordance with published response plan informing SO1 Security at the time or within 1 Working Day; and (d) demonstrate conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.91
	17.13	**Operational Security: Incident Management** The Contractor shall:	Schedule 4.1 - Security Section: 9.6 Compliance Approach

		(a) comply with the measures defined in the DBS Cyber Response Plan, and the DBS Incident Response Plan; (b) processes and procedures to manage security incidents are to be in place 100% of the time; (c) security incidents are to be reported in acceptable timescales and formats as detailed within the DBS Cyber Incident Response Plan. The Authority (SO1 Sy) is to be informed at the earliest opportunity, and within 1 Working Day; and (d) demonstrate conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.	to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.92
	17.14	**Personnel Security** The Contractor shall: (a) conduct personnel security activities (including personnel screening) to ensure that only those personnel who have a need to access the systems and data are able to do so including, but not limited to: (i) thorough enquiries into identity, nationality (including right to remain and work in the UK), previous employment record and a criminal records check covering both spent and unspent convictions; unspent convictions only are considered as part of the recruitment process through the Baseline Personnel Security Standard; (ii) National Security Vetting to an appropriate level dependent on the individual requirement of the role; (iii) supervision of personnel, including for Developed Vetting (DV) holders, an annual Security Appraisal of an individual's continuing suitability for clearance; (iv) processes for reporting changes in personal circumstance, and issues/incidents that could give rise to concerns as to an individual's loyalty, reliability or integrity; and (v) enhanced supervision or limited access to information, for individuals whose loyalty, reliability or trustworthiness is a concern and potentially a risk to sensitive assets or classified information; and (b) conduct personnel screening with the level of screening required dictated by access levels as agreed with the Authority (SO1 Sy) and the DBS Vetting Policy and require any Sub-Contractor to conduct the same screening requirements.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.93

	17.15	**Secure Development.** The Contractor shall: (a) ensure that services are designed and developed to identify and mitigate threats to their security. Security is to be considered as an important factor in all elements of system development; (b) provide evidence of the controls in place to ensure the security of the Service in response to a request from the Authority (SO1 Sy) within a timescale to be agreed; (c) ensure that system development adheres to a secure development standard or recognised good practice at all times; (d) review all new and evolving threats in the context of impact upon the Service; (e) carry out all development in line with industry good practice regarding secure design, coding, testing and deployment; and (f) ensure that 'Configuration Management' processes are in place to ensure the integrity of the solution through development, testing and deployment at all times.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.94, 9.6.98
	17.16	**Supply Chain Security** The Contractor shall: (a) ensure its supply chain satisfactorily meets all of the security principles required of Sub-Contractors in this Agreement and demonstrate to the Authority on request that the security controls which are applicable to the system are enforced through their supply chain; (b) maintain an asset database that contains configuration information against each assets, with the capability to identify the addition and removal of assets, and automatically record the configuration of a newly added asset, and alert the asset owner upon removal of a current asset; (c) have a comprehensive inventory of assets connected to the network; (d) manage the configuration of all connected devices by remote means; (e) ensure that records of each 'Dynamic Host Configuration Protocol' allocation and release are maintained for a period of 6 months; and (f) demonstrate supply chain security conformance with a recognised standard and any non-conformance is to be notified to the Authority (SO1 Sy) within 5 Working Days of discovery.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.95

SANS CONTROLS	18.1	**SANS Control 1 – Inventory of Authorised and Unauthorised Devices** The Contractor shall, using the Information Bearing Asset Register, actively manage (inventory, track and correct) all Hardware used within the IT Environment so that only authorised devices are given access and authorised, and unmanaged devices are found and prevented from gaining access.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.96, 9.6.97
	18.2	**SANS Control 2 – Inventory of Authorised and Unauthorised Software** The Contractor shall: (a) implement a service for managing software assets for the identifying network users and managing licensing, versioning and the prevention of the execution of unauthorised software; (b) maintain an automated database of all software assets (including all instances of Active Directory), to include version, patch, licence, patch and accreditation status. Applicable across all environments and operating systems; (c) implement a white listing system, whereby only known and approved software of a known configuration, patch and build are allowed to execute; and (d) run Software in a manner whereby it does not pose a threat to other applications.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.98
	18.3	**SANS Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** The Contractor shall ensure that the management of configuration and Releases are secure which shall include, but not be limited to: (a) standardised versions of applications where multiple instances are required with only required services running are to be deployed; (b) the integrity of all applications and data files are to be established; (c) where available, deploying secure methods of communication and connection between network management protocols; (d) monitoring the configuration of all Software; (e) maintaining Software Port Control, Allocation and usage are to be monitored; and (f) managing and deploying 'System Configuration Policies' and other associated objects.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.99
	18.4	**SANS Control 5 – Controlled Use of Administrative Privileges** The Contractor shall control the use of Administrative privileges for access to the IT Environment by performing the following:	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1:

		(a) ensuring that the actions of Privileged Users are managed and are traceable through protective monitoring. Ensure that the principle of least privilege is applied; (b) having knowledge of all accounts and applying particular measures to privileged account holders operating inside the boundary (such as 'Database Administrators'); (c) implement Two-Factor Authentication for DBS civil servant and Contractor Privileged Users; (d) subject all privileged accounts to automated inventory collation; (e) change all default passwords; (f) all privileged account management functions (creation, privilege allocation, promotion, demotion, suspension and deletion) are to be captured for protective monitoring; (g) permit all Privileged User account transactions on a ticket-by ticket basis; and (h) implement the security requirements contained in this Schedule within the cloud environment.	Baseline Security Requirements Paragraph: 9.6.100
	18.5	**SANS Control 6 – Maintenance, Monitoring and Analysis of Audit Logs** The Contractor shall provide maintenance, monitoring, and analysis of audit logs by performing the following: (a) support the capability of the 'Protective Monitoring System' including analysis of logs captured; (b) ensure that the 'Protective Monitoring System' always has access to at least two synchronised time sources; (c) validate the audit logs for all connected Hardware and Software devices and processes to ensure that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction; (d) where an application is capable of generating security audit logs, that capability such that is compliant with the protective monitoring requirement is to be activated to allow auditable activities to be recorded and made available to the 'Protective Monitoring System'; (e) ensure that the IT Environment systems record logs in a standardized format such as syslog entries or those outlined by the 'Common Event Expression' initiative; (f) if systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.101

		(g) ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed; (h) actively review any reports identifying anomalies in logs at the intervals to be agreed with the Authority (SO1 Sy); and (i) identify and bring to the attention of the Authority (SO1 Sy) any anomalous action, or action identified as being of a serious security nature, as soon as practicable.	
	18.6	**SANS Control 7 – Email and Web Browser Protection** The Contractor shall: (a) use only supported web browser and email clients; and (b) ensure that all software (including browser and email clients) is in-support, licensed and, where practical, accredited (e.g. the use of a 'Commercial Off The Shelf' product may be accredited rather than the product itself).	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.102
	18.7	**SANS Control 9 - Limitation and Control of Network Ports, Protocols, and Services** The Contractor shall provide limitation and control of network ports by doing the following: (a) manage all network ports within their area of responsibility; (b) deactivating all Network 'Terminal Access Ports' (TAPs) unless required for use; (c) monitor all Network TAPs for use and ensure that active ports are associated with a device; (d) any change in status of a network port is to be captured by protective monitoring; (e) removal or addition of an authorised device from a Network TAPs is to be alerted; (f) prevent any connection to a network port of a device that has not previously been authorised; and (g) whilst the network boundary will have protection, individual devices within the boundary are also to be protected within the capabilities of any operating system used.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.103
	18.8	**SANS Control 10 – Data Recovery Capability** The Contractor shall provide data recovery capability by continuing to apply the principles of backing up, restoration of data, and testing for capability to restore which are applied during Transition into Transformation.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.104

	18.9	**SANS Control 11 – Secure Configurations for Network Devices** The Contractor shall provide secure configurations for Network devices by doing the following: (a) implement secure configuration of the network devices in accordance with JSP440 and JSP604, taking guidance from ISS; (b) ensure it has the capability to compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organisation; (c) document the security configuration of firewalls, routers, and switches to facilitate Authority and Configuration Control board review; (d) ensure that any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system; (e) all new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, will be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need; (f) use automated tools to verify standard device configurations and detect changes. All alterations to such files will be logged and automatically reported to security personnel; (g) manage network devices using two-factor authentication and encrypted sessions; (h) install the latest stable version of any security-related updates on all network devices after appropriate testing has taken place to ensure non-interference with delivery; (i) ensure that all Network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access, such machine being: (i) isolated from the primary network; (ii) not connected to the internet; and (iii) not used for reading e-mail, composing documents, or surfing the Internet; and (j) manage the network infrastructure across network connections that are separated from the business use of that network, relying on	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.105

		separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	
	18.10	**SANS Control 12 – Boundary Defence** The Contractor shall implement effective boundary defence by performing the following: (a) implement and maintain an effective boundary defence in accordance with JSP440 and JSP604, will take advice on boundary protection from ISS. The security measures implemented for the network shall include the capability to deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists); (b) carry out periodic Tests by sending packets from logon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Testing should take place at least once between each SWG; (c) configure DMZ networks with monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network; (d) network-based IDS sensors shall be deployed on Internet and extranet DMZ systems and networks which will look for unusual attack mechanisms and detect compromise of these systems; (e) network-based IPS devices shall be deployed to complement IDS by blocking known bad signatures or the behaviour of potential attacks; (f) require all DBS privileged user login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication; (g) all enterprise devices remotely logging into the internal network shall be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (for example, those belonging to Sub-Contractors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.106

		(h) periodically scan for back-channel connections to the Internet that bypass the De-Militarised Zone (DMZ), including unauthorized Virtual Private Network (VPN) connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms; (i) deploy 'NetFlow' collection and analysis to DMZ network flows to detect anomalous activity; (j) endeavour to identify covert channels exfiltrating data through the firewalls; and (k) configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify Transmission Control Protocol (TCP) sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.	
	18.11	**SANS Control 13 – Data Protection** The Contractor shall: (a) implement measures to comply with all data protection provisions as detailed in this Agreement and apply all SANS Security Control 13 data protection measures; (b) ensure that those measures are carried through in to transformation, and ensure that increased capability of transformation is reflected in the manner in which the data protection measures are implemented; (c) perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls; (d) deploy an automated tool on the network perimeter that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel; (e) conduct periodic scans of servers using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text; (f) configure systems so that they will not write data to USB tokens or USB hard drives and maintain an inventory of all authorized devices must be maintained;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.107

		(g) use network-based DLP solutions to monitor and control the flow of data within the network; (h) report any anomalies that exceed the normal traffic patterns (as specified by the Authority); (i) any anomalous activity is to be investigated in accordance with the incident management process; (j) monitor all traffic leaving the organization and detect any unauthorized use of encryption; (k) block access to known file transfer and e-mail exfiltration websites; and (l) deploy host-based data loss prevention (DLP) to enforce Access Control Lists (ACLs) even when data is copied off a server.	
	18.12	**SANS Control 14 – Controlled Access** The Contractor shall implement controlled access based on role and the principle of 'Need to Know' by performing the following: (a) apply the access control methods and measures through SANS Security Control 14 and ensure that those measures are maintained throughout the Term, and ensure that any increased capability through Transformation is reflected in the manner in which the data protection measures are implemented; (b) segment the network based on the label or classification level of the information stored on the servers; (c) locate all sensitive information on separated Virtual Local Area Networks (VLANS) with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfil their specific responsibilities; (d) ensure that all communication of sensitive information over less-trusted networks is encrypted; (e) ensure that all network switches enable Private VLANs for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighbouring systems; (f) ensure that all information stored within IT Environment shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.108

		(g) ensure that sensitive information stored on the IT Environment shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information; (h) enforce detailed audit logging for access to non-public data and special authentication for sensitive data; and (i) ensure that any archived data sets or systems that have not been accessed for 12 months shall be removed from the live environment. Such data sets or systems completely virtualized and powered off until needed and shall only be used as standalone systems (disconnected from the MoD Core Network) by the business unit needing to occasionally use the data set or system.	
	18.13	**SANS Control 18 – Application Software Security** The Contractor shall apply NCSC guidance for secure development and deployment to the implementation of application software security by performing the following: (a) ensure that for all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations; (b) protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks; (c) for applications that are not web-based, deploy specific application firewalls if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed; (d) ensure that for in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats; (e) Test all in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.109

		basis. In particular, input validation and output encoding routines of application software should be reviewed and tested; (f) ensure 'Output Sanitisation' by not displaying system error messages to End Users; (g) maintain the Production Environments separate from any non-Production systems. Developers should not typically have unmonitored access to the Production Environment; (h) for applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested; (i) ensure that all software development personnel receive training in writing secure code for their specific development environment; and (j) for in-house developed applications, ensure that development artefacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.	
	18.14	**SANS Control 19 – DART** The Contractor shall record and maintain system application dependencies on the 'Defence Assurance Risk Tool' at all times.	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.110
	18.15	**SANS Control 20 – Data Loss Prevention** The Contractor shall: (a) implement, promote, and enable data loss prevention at all times by utilising all available means within JPA and its associated applications to undertake end-to-end monitoring and data export attribution to individual account level. Such a solutions shall: (i) be fully integrated into SOC and security technologies in order that 'normal' behaviours (as defined by the Authority) can be determined and monitored; (ii) enable limits/constraints applied to prevent or mitigate 'abnormal' behaviour (as defined by the Authority); and (iii) use meta-data to identify the type/nature of material populating any given field and, whenever a non-database document is saved, the requirement to set meta-data should be enforced utilising a taxonomy agreed with the Authority;	Schedule 4.1 - Security Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.111

		(b) undertake end-to-end monitoring and data export attribution, to individual account level by utilising greater technical data management to: (i) define data types and locations; (ii) define expected data flows; (iii) enable data export (via printer or other electronic means) by authorised users to be monitored with a view to managing, controlling and if necessary limiting data export; (iv) explore and if successful introduction of on screen messaging to warn users of the handling procedures required and possible consequences of exporting large volumes of sensitive personal data; (v) fully integrate the SOC monitoring and security technologies develop and support DLP policies; and (vi) define work flow and incident handling processes.	
SECURITY AND INFORMATION GOVERNANCE	19	The Contractor shall provide support to the 'Security and Information Assurance Governance' structure by performing the following: (a) coordinate, prepare and attend 'Security and Information Assurance Governance' meetings in coordination with the Authority (DBS ITS SO1 Sy) to schedule to be agreed with the Authority (DBS ITS SO1 Sy) on the Effective Date and reviewed annually. At each such meeting, the Contractor will be represented by the ASM and SMEs (as appropriate). These will include, but not be limited to, the following meetings: (i) a 'Security Working Group' (SWG) meeting every 6 weeks or as required by the Authority; (ii) a 'Assurance Strategy' meeting every 2 weeks or as required by the Authority; (iii) a 'Security and IA Risk Review' meeting every prior to each SWG or as required by the Authority; (iv) an 'ITSHC' routine and ad hoc meetings as agreed with the Authority (DBS ITS SO1 Sy); and (v) an 'Information Asset Owners Working Group' meeting as required by the Authority (DBS).	Schedule 4.1 - Security Section: 9.3 Overview of the Account Security Service Proposals Paragraph: 9.3.9 Section: 9.6 Compliance Approach to Schedule 2.4 Appendix 1: Baseline Security Requirements Paragraph: 9.6.58
Schedule 6.2 (Testing)			
INTRODUCTION	1.1	The Authority requires that the Contractor demonstrates in accordance with this Schedule 6.2, that the Deliverables meet the Service Requirements or, in the case of a Deliverable to be provided pursuant to	

		a Change Request, the Change Authorisation Note, and that the introduction of such Deliverable will not prejudice the effectiveness, operational integrity and/or security of the Services or the Authority Systems. Where the introduction of a Deliverable prejudices the effectiveness, operational integrity and/or security of the Services or the Authority Systems, the Contractor will notify the Authority of the same as soon as it becomes aware of such occurrences.	
	1.2	This Schedule 6.2 sets out the procedures: (a) that apply to the assurance of Documentation; (b) for Testing and assurance of Deliverables; (c) for Testing and assurance of Changes to existing Authority Systems; (d) for Testing and assurance of new Systems and Services; and (e) the issue of Milestone Achievement Certificates.	Schedule 4.1 Organisation and Governance Section: 7.9 Testing: Test Strategy
	1.3	The Testing Procedures shall apply to: (a) any Documentation Deliverables as agreed with the Authority; (b) any Deliverables to be developed and/or supplied by the Contractor as agreed with the Authority. For the avoidance of doubt this includes any Contractor-supplied updates to hardware and software (including patches, updates and fixes, and all systems infrastructure and applications software updates, firmware patches, software patches and fixes); (c) any Change (as set out in the relevant Contract Change Authorisation Note) that has a potential impact on the ability of the Authority to comply with its obligations under this Agreement; and (d) any new system or service delivered by reason of the transformation programme.	
	1.4	The Testing Procedures described in this Schedule 6.2 shall be followed by the Authority and the Contractor unless agreed otherwise.	
RISK	2.1	The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not: (a) operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Authority's requirements for that Deliverable or Milestone; or (b) affect the Authority's right subsequently to issue a notice of a Defect against all or any element of the relevant Deliverable to which a Test Certificate relates, and the Contractor shall be responsible for the costs of remedying any such Defect.	

	2.2	Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Contractor shall remain solely responsible for ensuring that: (a) the Contractor Solution as designed and developed is suitable for the delivery of the Services and meets the Authority Requirements; (b) the Services are implemented in accordance with this Agreement; and (c) each Target Performance Level is met from the relevant Operational Service Commencement Date.	
PART 2: TESTING AND ASSURANCE PROCEDURES FOR DOCUMENTARY DELIVERABLES INTRODUCTION TO ASSURANCE PROCEDURES FOR DOCUMENTARY DELIVERABLES	1.1	Part 2 of this Schedule 6.2 specifies the Testing Procedures applicable to Documentary Deliverables.	
	1.2	The Contractor shall ensure that all Documentary Deliverables are identified in the relevant Assurance Plan including the timing of their delivery and review.	
	1.3	The Testing Procedures for Documentary Deliverables are designed to enable the Authority to review draft Documentary Deliverables produced by the Contractor against agreed Assurance Criteria, and for the Authority to satisfy itself of the contents of such drafts subject to any required changes being made.	
	1.4	The Contractor shall consult with the Authority and take into account any reasonable comments and recommendations made by the Authority in respect of a Documentary Deliverable.	
	1.5	The Testing Procedures for Documentary Deliverables shall commence with the Parties' agreement of the Deliverable Description for the Documentary Deliverable in accordance with paragraph 2. The Deliverable Description shall set out the applicable Assurance Criteria.	
AGREEMENT OF DELIVERABLE DESCRIPTION FOR DOCUMENTARY DELIVERABLES	2.1	Where a Documentary Deliverable is submitted by the Contractor for assurance by the Authority, the Contractor shall develop a draft Deliverable Description: (a) in the format specified at Appendix 1 to this Schedule; and	

		(b) which provides full details in respect of the matters set out in Appendix 1 (including the Assurance Criteria), and shall provide the draft Deliverable Description to the Authority for review in accordance with the Assurance Plan.	
	2.2	The Authority shall review the draft Deliverable Description in order to determine whether it is in the format specified at Appendix 1 to this Schedule and whether the Assurance Criteria contained within the Deliverable Description reflect the objective of the Documentary Deliverable.	
	2.3	Where the draft Deliverable Description meets the requirements set out in paragraph 2.2, the Authority shall notify its agreement of the Deliverable Description in writing to the Contractor.	
	2.4	Where the draft Deliverable Description does not meet the requirements set out in paragraph 2.2, the Authority shall notify the Contractor, specifying the reasons why the draft has not been agreed. In this event, the Contractor shall liaise with the Authority to understand the Authority's concerns. Following this, the Contractor shall complete the necessary changes and shall issue a revised draft Deliverable Description within five (5) Working Days of the Authority's notification pursuant to this paragraph 2.4 (or such timetable as may be agreed in advance and by exception between the Parties), with all the changes clearly highlighted, to the Authority for review.	
KEY ROLES IN REVIEWING DOCUMENTATION DELIVERABLES	3.1	For each Documentary Deliverable review, the Contractor shall appoint a suitably qualified and authorised representative to manage the assurance of each draft Documentary Deliverable.	
AGREEMENT OF ASSURANCE PLAN FOR DOCUMENTATION DELIVERABLES	4.1	The Authority and the Contractor shall agree (as soon as is reasonably practicable) an Assurance Plan, which shall be consistent with the overall timescale for development and approval of any Documentary Deliverables set out in the Transition Plan and/or the Transformation Plan or any timescales set out in any Change Authorisation Note.	
	4.2	The Assurance Plan shall record the following dates for each of the above Documentation Deliverables: (a) the First Draft Delivery Date; (b) the date by which the Authority will notify the Contractor of the outcome of its review of the first draft of the Documentation Deliverable and provide any review comments; (c) the date by which the Authority and the Contractor will meet to review the Authority's comments;	

		(d) an estimated date by which the Contractor shall submit a revised draft Documentary Deliverable; (e) an estimated date by which the Authority shall check the revised draft; and (f) the planned date for approval by the Authority in respect of any Documentary Deliverable ("Planned Assurance Date").	
REVIEW PROCEDURE FOR DOCUMENTARY DELIVERABLES	5.1	The Authority and the Contractor shall each conduct the review in accordance with the Assurance Plan and the timescales specified therein.	
	5.2	The Contractor shall not submit the draft Documentation Deliverable for review by Authority without first satisfying itself that the draft Documentation Deliverable: (a) has been developed in accordance with the format, scope and Assurance Criteria specified in the applicable Deliverable Description; (b) is clearly written, in language that those Parties who will need to refer to the document should be able to understand; (c) does not refer to any document not provided to, or in the possession of, the Authority unless the Parties have previously agreed that such document is not required to be provided; (d) effectively draws upon the necessary expertise and reflects Good Industry Practice; (e) is complete, with an appropriate level of detail and any relevant cross-references; and (f) has no obvious errors of spelling, grammar, numbering or order, duplications or omissions.	
	5.3	The Authority shall review the draft Documentary Deliverable to objectively determine whether it meets the applicable Assurance Criteria or not, and shall notify the Contractor of the outcome of this review, in accordance with the Assurance Plan.	
	5.4	If the Authority's review determines that the draft meets all the applicable Assurance Criteria by or before the Planned Assurance Date, the review shall be concluded at this point, and the Authority shall promptly issue to the Contractor a Test Certificate.	
	5.5	If all applicable Assurance Criteria are not met by the Planned Assurance Date, the Authority shall notify the Contractor in writing of this and without prejudice to the Authority's other rights and remedies particularly as set out in Clause 6 (Transition and Transformation) of this Agreement, the	

		Contractor shall re-submit the relevant Documentary Deliverable for assurance as soon as possible but in any event no later than five (5) Working Days of the Authority's notification pursuant to this paragraph 5.5.	
	5.6	The Contractor shall ensure that any changes in respect of any Documentary Deliverable which has been re-submitted for assurance pursuant to paragraph 5.5 are clearly highlighted.	
TEST QUALITY AUDIT	6.1	Without prejudice to its rights pursuant to Clause 14 (Records, Reports, Audits & Open Book Data), the Authority may perform on-going quality audits in respect of any part of the Testing (each a “Testing Quality Audit”) subject to the provisions set out in the agreed Quality Plans.	
	6.2	The focus of the Testing Quality Audits shall be on: (a) adherence to an agreed methodology; (b) adherence to the agreed Testing process; (c) adherence to the Quality Plan; (d) review of status and key development issues; and (e) identification of key risk areas.	
	6.3	The Contractor shall ensure that adequate responses to a Testing Quality Audit are provided within 10 Working Days (or such longer period as the Authority may agree) of the Authority's conclusion of any such audit.	
	6.4	The Authority will give the Contractor at least 5 Working Days' written notice of the Authority’s intention to undertake a Testing Quality Audit and the Contractor may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Contractor’s reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Authority will materially and adversely impact the Transition Plan and/or Transformation Plan.	
	6.5	A Testing Quality Audit may involve document reviews, interviews with the Contractor Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Authority witnessing Tests and demonstrations of the Deliverables to the Authority. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Contractor and the Authority on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Contractor shall provide all reasonable necessary assistance and access to all relevant documentation required by the Authority to enable it to carry out the Testing Quality Audit.	

	6.6	If the Testing Quality Audit gives the Authority concern in respect of the Testing Procedures or any Test, the Authority shall: (a) discuss the outcome of the Testing Quality Audit with the Contractor, giving the Contractor the opportunity to provide feedback in relation to specific activities; and (b) subsequently prepare a written report for the Contractor detailing its concerns, and the Contractor shall, within a reasonable timeframe, respond in writing to the Authority's report.	
	6.7	In the event of an inadequate response to the Authority's report from the Contractor, the Authority (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate or conditional Milestone Achievement Certificate, as appropriate) until the issues in the report have been addressed to the reasonable satisfaction of the Authority.	
PART 3: TESTING PROCEDURES FOR DELIVERABLES OTHER THAN DOCUMENTARY DELIVERABLES INTRODUCTION TO TESTING PROCEDURES FOR DELIVERABLES OTHER THAN DOCUMENTARY DELIVERABLES	1.1	The Contractor shall ensure that the Test Strategy provides the high level direction for the approach to testing of Deliverables and the Test Plan identifies what Deliverables shall be subject to the Testing Procedures, when testing will commence and finish and the acceptance criteria.	Schedule 4.1 Organisation and Governance Section: 7.9 Testing: Test Strategy
	1.2	The Testing Procedures for Deliverables are designed to demonstrate that: (a) the Deliverables meet the Test Success Criteria; (b) any changes to the Deliverables (as set out in any relevant Change Request do not have an adverse impact on the existing Deliverables or to the Authority's ability to comply with its obligations in this Agreement; and (c) any changes to the Deliverables do not have an adverse impact on business continuity and the provision by the Contractor of the Services.	
	1.3	The Testing Procedures for the Deliverables are outlined below and cover the: (a) preparation and agreement of the Test Strategy: (b) preparation and agreement of the Test Plan;	

		(c) general Test procedures for the Deliverables; (d) Test Stages; (e) defect identification and management processes; and (f) consequences of Test Success and Test Failure.	
	1.4	The Contractor shall provide a system to record Defects identified during Testing, as they occur, and manage the Defect to resolution, or refer the Defect to the [Problem Management System] at the end of a Testing cycle (such system being the "Defect Management System"). The Defect Management System is to be deployed from the Operational Service Commencement Date. The Contractor shall: (a) ensure that all Defects found during a Testing phase are logged in the Defect Management System; (b) implement a Defect Management System (including establishing the Defect Review Board) that supports the Problem Management Policies and Procedures defined in Schedule 2.1, Part 12 (IT Service Management) and must ensure that the Defect Management System is available to the Authority at all times; (c) the Defect Management System shall record details of the Defect found, it is to include, but is not limited to: (i) the ability to create a unique defect identifying number; (ii) details of the person who identified the Defect; (iii) a description of the Defect; (iv) a category of Defect; (v) the priority for rectifying the Defect; and (vi) details of IT hardware and software used during the Test.	Schedule 4.1 Organisation and Governance Section: Test Tooling Paragraph: 7.13.4
	1.5	The Contractor shall provide an integrated Test toolset ("the Test Toolset") which is to be deployed from the Operational Service Commencement Date. Test management tools are used to facilitate regular software development activities, automate & manage testing activities. The Test Toolset shall include, but is not limited to: (a) Performance, Functional and Load test tools: (b) a testing administration facility with link to the Defect Management System; and (c) the Testing tools shall integrate with the Problem Management process and toolset as required in Schedule 2.1, Part 12 (IT Service Management) for those Defects which remain unresolved after Testing has completed.	Schedule 4.1 Organisation and Governance Section: 7.13 Test Tooling
	1.6	The Contractor shall, no later than 40 Working Days after the Operational Services Commencement Date, provide an inventory of Tests	Schedule 4.1 Organisation and Governance

		Environments and Maintenance and Support Environments, in order to support optimisation across the estate in accordance with SACM Policies and Procedures.	Section: 7.14 Testing: Defect Management Paragraph: 7.14.10
	1.7	The Contractor shall, throughout the Term, maintain the inventory of Test Environments and Maintenance and Support Environment. The Contractor shall, no later than 10 Working Days after the expiry of each Quarter, provide a copy of the inventory of Test Environments and Maintenance and Support Environments and details of its maintenance activities during that Quarter (the "Test Environment Inventory") for the Authority's review. The Authority shall review and, acting reasonably, provide its approval or comments in respect of the Test Environment Inventory within 5 Working Days. In the event that the Authority provides comments on the Test Environment Inventory, the Contractor shall provide an updated draft taking into account the Authority's comments. The Contractor shall, in the event of any Change, review and update the Test Environment Inventory within 5 Working Days following such Change coming into full force and effect.	Schedule 4.1 Organisation and Governance Section: 7.14 Testing: Defect Management Paragraph: 7.14.10
	1.8	In addition to its obligations set out in paragraph 1.5 above, the Contractor shall, from the Operational Service Commencement Date: (a) provide a Testing Toolset to support all test activities across the Military Personnel and Veterans Reporting Platform and comply with available open testing standards; and (b) provide the Authority's nominated users with access (not to exceed 10) to the Standard Testing Toolset in accordance with NFRs.	Schedule 4.1 Organisation and Governance Section: 7.14 Testing: Defect Management Paragraph: 7.14.10
PREPARATION AND AGREEMENT OF THE TEST STRATEGY	2.1	Within 40 Working Days after the Effective Date, the Authority and the Contractor shall, each acting reasonably, agree a Test Strategy ("the Test Strategy") to define and regulate testing across all elements of Military Personnel and Veterans Services. The Test Strategy shall define the approach for the implementation and verification of Deliverables. The Contractor shall ensure that the Test Strategy is maintained throughout the Agreement.	Schedule 4.1 Organisation and Governance Section: 7.13 Testing: Test Strategy Paragraph: 7.9.6
	2.2	The timings for the agreement of the Test Strategy shall be as follows: (a) 40 days prior to the Operational Service Commencement Date, provide a draft Test Strategy to the Authority's Test Manager; (b) 30 days prior to the Operational Service Commencement Date, agree the Test Strategy with the Authority; (c) from the Operational Service Commencement Date, the Test Strategy shall come into force; and	

	2.3	On each anniversary of the Operational Service Commencement Date, the Parties shall review the Test Strategy.	
	2.4	The Test Strategy shall include (but is not limited to) the following: (a) Scope and objectives; (b) Roles and responsibilities; (c) Communication and status reporting; (d) Quality gates; (e) Critical success factors; (f) Entry and Exit Criteria; (g) Test Deliverables; (h) Industry standards to adhere to; (i) Test techniques and tools; (j) Testing measurements and metrics; (k) Risks and mitigation; (l) Defect reporting and tracking; (m) Change and configuration management; and (n) Training plan.	
	2.6	The Test Plan shall be updated from time to time by the Contractor in accordance with a timetable to be agreed by the Parties.	
PREPARATION AND AGREEMENT OF THE TEST PLAN	3.1	The Contractor shall identify a dedicated Test co-ordinator for the purpose of co-ordinating its responsibilities in the preparation and agreement of the Test Plan, and the preparation and undertaking of Tests.	Schedule 4.1 Organisation and Governance Section: 2.9 Effective tools and techniques for Relationship Management Plan Paragraph: 2.9.3 - 2.9.4
	3.2	The Authority and the Contractor shall (as soon as is reasonably practicable, but in any event no later than ten (10) Working Days (or such shorter period as the Parties may, acting reasonably, agree) prior to any date upon which the relevant Deliverables are to be submitted for Testing, agree a Test Plan, including Product Test Plans and Release Test Plan which shall be consistent with the timescales set out in the Transition Plan and/or the Transformation Plan, or any Change Authorisation Note (as applicable).	Schedule 4.1 Organisation and Governance Section: 7.10 Testing: Test Plans Paragraph: 7.10.3
	3.3	The Test Plan shall record the start and end dates all Test Stages listed at paragraph 8.	
	3.4	The Contractor shall ensure that the Test Plan includes, but is not limited to, the following: (a) Test approach;	

		(b) Test Specifications; (c) Test Data; (d) Test Stages; (e) Entry criteria; (f) expected results; (g) acceptance criteria; (h) error/Defect identification processes; (i) error/Defect resolution plans; (j) Test environment configurations; (k) configuration of elements passing through the Test (including which versions of software and hardware are to be Tested); (l) details of any tools used, including automated Test tools; and (m) When testing the Military Personnel and Veterans Reporting Platform, provide definitions of updates and patches being applied and their expected impacts, and the explanation of such impacts.	
	3.5	The Contractor shall ensure that the Test will be conducted in accordance with the Security Plan.	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.15
	3.6	The Contractor shall consult the Authority regarding the preparation of the Test Plan and take into account any reasonable comments and recommendations made by the Authority in respect of the Test Plan. In particular, the Contractor shall consult the Authority regarding the acceptability of the proposed scope, duration and timing of the Test, proposed Test Stages, proposed sources of Test Data, Test environments and any proposed Authority involvement in preparing for, witnessing, monitoring or undertaking the Tests.	Schedule 4.1 Organisation and Governance Section: 7.10 Testing: Test Plans Paragraph: 7.10.2
	3.7	The Authority reserves the right (subject to paragraph 7.6(a)) to create and conduct its own Tests within the Test process, including developing associated test specifications and directly managing such Tests, which the Authority may consult the Contractor on. The Contractor shall take account of and incorporate the Authority's reasonable requirements in this respect when preparing the Test Plan.	
	3.8	The Authority reserves the right to provide Test Data (in an agreed format) for use within the Test process. The Contractor shall consider and comply with any of the Authority's reasonable requirements in this respect when preparing the Test Plan. The Contractor shall provide all	

		other Test Data that is required to allow the Test to be performed, and shall ensure that such Test Data is both relevant and adequate for the purposes of the Tests for which it is being used.	
	3.9	The Contractor (and the Authority where it has supplied the Test Data) shall ensure that the proposed sources and use of Test Data would cause neither the Contractor nor the Authority to breach any of its applicable obligations under Data Protection Legislation. In particular, the Contractor shall not use any live data for Test purposes without the Authority's prior written consent.	
	3.10	The Contractor shall design the Test Plan to ensure as far as is reasonably possible that the proposed Tests minimise any potential disruption to the Services and the Authority's business.	
	3.11	In planning any Test, the Authority and the Contractor shall consider and agree what third party involvement is appropriate. The Contractor shall consult such third parties regarding the planning accordingly.	
	3.12	Where third parties are involved in a Test, the Contractor shall provide them with all reasonably necessary assistance and information in connection with the conduct of that Test.	
	3.13	Where the Contractor, in meeting its obligations under this Schedule 6.2, consults or otherwise directly works with one or more third parties identified in paragraph 3.11, the Contractor shall provide the Authority with reasonable visibility of such interaction.	
TEST READINESS REVIEW	4.1	Prior to the commencement of Testing, the Contractor shall, in conjunction with the Authority, conduct a test readiness review to ascertain if Testing can commence.	
	4.2	The test readiness review shall include, but is not limited to, the following: (a) assess Test objectives; (b) Test methods and procedures; (c) scope of Tests; and (d) confirmation that adequate resources have been identified and allocated to the Test.	
GENERAL TESTING PROCEDURES FOR DELIVERABLES	5.1	The Parties shall conduct the Test in accordance with their respective obligations under the Test Plan and the timescales specified therein.	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.15
	5.2	The Contractor shall provide all reasonably necessary assistance and information in connection with the conduct of the Test.	Schedule 4.1 Organisation and Governance

			Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.7
	5.3	The Contractor shall: (a) undertake all Testing identified in response to a Change Request or as covered within a Product or Release Test Plan and as detailed within Schedule 6.2 (Testing Procedures) ensuring that the testing scope, validity and coverage meets the criteria of the testing strategy and test plan; (b) make all test scripts available to the Authority (Test Manager, Change Manager, Business Process leads, Technical Assurance) within 1 Working Day of request; and (c) provide to the Authority Test Manager a report on test script executions at a frequency to be agreed in the Test Strategy, across a timeframe to allow run rates to be established. Reports are to include but not be limited to: (i) Test runs; (ii) Test re-runs (iii) Test success; (iv) Test failures; (v) Test rejects; and (vi) Tests outstanding.	Schedule 4.1 Organisation and Governance Section: 7.6 Change Delivery Paragraph: 7.6.5
	5.4	The Contractor shall update the automated scripts of the Regression Test and Performance Test to reflect the alterations introduced by each Change Release. Updates shall be made and tested prior to the next scheduled Release.	Schedule 4.1 Organisation and Governance Section: 7.5 Change Initiation, Impact and Approval/Rejection Paragraph: 7.5.5
	5.5	The Contractor shall, in respect of all Releases onto the Military Personnel and Veterans Reporting Platforms (or other change delivery method) undertake automated regression testing on all Authority defined dashboards and deliver results to the Authority (Authority Test Manager Military Personnel MI Manager).	
	5.6	The Contractor shall undertake Tests in accordance with Good Industry Practice and any agreed methods, codes and/or Standards set out in Schedule 2.3 (Standards) and processes identified in this Agreement. From the Operational Service Commencement Date, the Contractor shall provide and maintain an automated system for the recording and management of errors and / or defects raised during the Testing phases	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.3

		of each Change which shall be delivered in accordance with all NFRs and shall provide access to the Authority's nominated personnel from Authority devices.	
	5.7	The Contractor shall, on the date specified in the Test Plan for the commencement of the Test, perform the following, as may be required in the Test Plan: (a) provide documentary evidence that the Contractor has in place the necessary staff, accommodation, equipment, facilities and other resources to develop and/or supply the Deliverables and to implement any changes pursuant to a Change Authorisation Note and that the Entry Criteria have been met; (b) demonstrate to the Authority, by means of visits by the Authority to the Contractor's premises and/or those of third parties (in both cases where those premises are used for or connected with the provision of the Services), interviews with any the Contractor Personnel, inspection of equipment and facilities or other means, that the Contractor has in place the necessary personnel, accommodation, environments, equipment, facilities and other resources to develop and/or supply the Deliverables and to implement any changes pursuant to a Change Authorisation Note; and (c) undertake the Test, or activities required in connection with the Test and implementing changes in accordance with any Change Authorisation Note.	
	5.8	The Contractor shall set up and coordinate the support for the Authority User Acceptance Testing.	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.12.2 - 17.12.5
	5.9	The Authority requires the Contractor to provide the Authority with access to: (a) the Test Management and Defect Management tools for the Authority's use for the purpose of User Acceptance Testing; and (b) read access to the Contractor Test Management and Defect Management tools, to provide the Authority with visibility during Test Stages. The Contractor shall take account of the Authority's requirements in this respect when preparing the Test Plan.	Schedule 4.1 Organisation and Governance Section: 7.12 Testing: Release Level Activities Paragraph: 7.12.4

	5.10	Unless otherwise agreed between the Authority and the Contractor and specified in the Test Plan, the Contractor shall provide the Test environments required for all Test Stages and shall ensure that the Test environments simulate the live environment as far as is reasonably practicable for each Test Stage.	Schedule 4.1 Organisation and Governance Section: 7.14 Testing: Defect Management Paragraph: 7.14.7
	5.11	The Contractor shall provide the Authority with access to a Test environment containing all the Changes scheduled for a Release and deliveries, in order to enable Authority User Acceptance Testing to be conducted, within the following timescales: (a) for Major Releases, 40 Working Days prior to such release; and (b) for all other Releases, within a timescale to be agreed with the Authority.	
	5.12	The Contractor shall make available the Test environment for Testing in accordance with all NFRs (as set out in Appendix 1 of Annex M to Schedule 2.1) during the testing period, except with prior approval of the Authority Test Manager and for the following durations: (a) As set out in Annex M, serial M54, for a Major Release, no less than 10 Working Days; and (b) for all other Releases, such period as agreed between the Parties or if no such period if agreed 10 Working Days.	
	5.13	For all Military Personnel &Veterans Reporting Platform User Acceptance Testing instances, within 24 hours of deploying a Change into the User Acceptance Testing environment, provide to the Authority (Military Personnel MI Manager) a copy of the MP&VRP configuration metadata.	
	5.14	The Contractor shall, no later than 20 Working Days prior to the start date for the User Acceptance Testing (as set out in the Impact Assessment), deliver to the Authority (Military Personnel MI Manager) an impact notification report In accordance with Paragraph 7.5 of Schedule 8.2 (Change Control).	
	5.15	Unless otherwise agreed between the Authority and the Contractor and specified in the Test Plan, the Contractor shall provide the Test environment that is accessible from the Authority IT infrastructure, for use by the Authority during the Authority User Acceptance Test Stage.	
	5.16	The environment provided for Authority User Acceptance Testing shall contain all of the scheduled Changes 40 Working Days prior to a Major Release, or as agreed with the Authority Test Manager. The Contractor shall ensure that the Authority User Acceptance Testing environment is maintained and simulates the live environment as far as is reasonably	

		practicable. It is to contain non-obfuscated data only, unless otherwise agreed with the Authority. The Test environment shall be provided to the Authority for the User Acceptance Testing no later than 10 (ten) Working Days prior to the commencement of that Test Stage.	
	5.17	The Testing environment provided for Authority User Acceptance Testing shall be available in accordance with all NFRs set out in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M1 (Technical Applications) to Schedule 2.1 (Services Description) during the Testing period (as laid down in the Test Plan), except with prior approval of the Authority Test Manager.	
	5.18	The Authority shall review any documentary evidence provided by the Contractor and/or attend any demonstrations for the purposes of the Test, and/or conduct Tests, as specified in the Test Plan.	
	5.19	The Contractor shall, no later than 1 day (or such other period as may be agreed with the Authority – acting through any of the Authority Change Manager, Authority Business Subject Matter Expert or Authority Test Manager - prior to the date on which any Change is scheduled to "go-live", facilitate Field Acceptance Testing. The facilitation by the Contractor shall include but not be limited to the provision of technical support during and outside working hours, as required by the Authority.	
TEST WITNESSING	6.1	In respect of all Tests undertaken by the Contractor, the Authority shall have the right to have reasonable numbers of observers attend and observe such Tests. Where third parties are required to attend and observe a Test, the Contractor shall permit a reasonable number of observers from that third party to attend and observe the Test, provided that such third party complies with applicable security and confidentiality requirements.	Schedule 4.1 Organisation and Governance Section: 7.10 Testing: Test Plans Paragraph: 7.10.4
	6.2	In respect of all Tests that are being undertaken by the Contractor, the Contractor shall provide the Authority, and any Test Witnesses that are to observe such Tests, with reasonable notice of which Tests are being carried out on which days. Unless otherwise specified in the Test Plan, reasonable notice will be a minimum of ten (10) Working Days.	
	6.3	The Test Witnesses may produce and deliver their own, independent reports on Testing, which may be used by the Authority to assess whether the Tests have been Achieved.	
	6.4	The Test Witnesses may raise Test Issues on the Defect Management System in respect of any Testing.	

TEST SPECIFICATION	7.1	Save as otherwise specified in the Test Plan and subject to [paragraph 13.2], the Contractor shall develop Test Specifications for each of the Tests, which the Contractor shall make available both to the Authority and to any third parties involved in a Test.	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.7 Section: 7.13 Test Tooling Paragraph: 7.13.1
	7.2	If the Test Plan specifies that the Authority is developing Test Specifications, the Authority shall consult with the Contractor regarding the development of such Test Specifications and shall make the Test Specifications available to the Contractor.	
	7.3	If the Contractor is developing Test Specifications for User Acceptance Testing, the Contractor shall consult with the Authority to ensure that the proposed Test Specifications are acceptable to the Authority.	
	7.4	If the Contractor is developing Test Specifications for any other Tests that directly involve the Authority and/or any third parties, in preparing for, monitoring or undertaking the Tests, the Contractor shall consult with the relevant parties regarding the development of the Test Specifications.	
	7.5	The party developing the Test Specification shall ensure that it is consistent in all respects with the agreed Test Plan.	
	7.6	Each Test Specification shall include: (a) identification of the Test Stage that the Test is part of (including any additional Test Stages and/or other Test Stages which will be conducted by the Authority and in respect of which the Authority has provided written notification to the Contractor); (b) the scope of the Test including the purpose of the Test and the Milestone or Key Milestone (if any) to which it relates; (c) any identifiable risks associated with either the Test Strategy, Test scope or Testing methods; (d) the role of, and any dependencies on, the Authority and/or any third party with regard to the Test; (e) relevant Test scripts (including a detailed procedure for the Test to be carried out); (f) specification of the required Test Data, including its accuracy, quality source, scope, volume and management, a request (if applicable) for relevant Test Data to be provided by the Authority, and the extent to which it is equivalent to live data;	

		(g) The Authority reserves the right, in respect of testing of the Military Personnel and Veterans and Reporting Personnel platforms, to require regression testing on all Authority-defined dashboards and reports which will be agreed as part of the Test Plan; (h) Test environment(s) to be provided and utilised; (i) Entry Criteria and Exit Criteria including any Error Thresholds; (j) expected outcome of the Test including a mechanism to be used to capture and record Test results and a method to process Test results to establish their content; (k) Test resources; and/or (l) the Test Success Criteria.	
TEST STAGES	8.1	For each Test, the Contractor shall consult with the Authority to establish what Test Stages are required. The Authority reserves the right to require any combination (or all) of the following Test Stages to be undertaken, and the Contractor shall incorporate the Authority's reasonable requirements in this respect into the Test Plan: (a) Unit Test: to be undertaken by the Contractor to ensure that the functions of the Deliverable are compliant with any relevant specification; (b) System Test: to be undertaken by the Contractor to ensure that the Deliverable operates in line with specified functional and non-functional requirements, including compatibility and security requirements; (c) Integration Test: to be undertaken by the Contractor to ensure that the Deliverable integrates and operates successfully, in accordance with the specified requirements, including compatibility and security requirements (including penetration Testing where agreed); (d) Performance Test: to be undertaken by the Contractor to determine that the Deliverable is capable of meeting contracted performance and volumetric requirements across expected load ranges; capable of being replicated, supplemented or otherwise expanded; together with data extraction, data validation, transform and load testing; (e) User Acceptance Test: to enable the Authority to satisfy itself that the functionality and performance of the Deliverable and/or integrated Deliverable meets its specified requirements; (f) Regression Test: the Contractor shall re-test Deliverables following modification, repair or upgrade to ensure that faults have not been introduced or uncovered as a result of the changes made.	TEST STAGES

		Regression Testing shall also cover Deliverables not directly affected by the modification, to ensure that no unspecified side effects have been caused by the changes; and/or (g) Field Acceptance Testing: a final assurance check that the JPA process changes being delivered will work as expected on the live system. Not all but selected JPA process changes (due to be delivered in a Release) will be checked at the end of delivery weekend, just ahead of the live JPA system being brought back up. The Authority shall be responsible for undertaking this Testing.	
	8.2	The Contractor shall conduct the Test Stages in accordance with the timescales defined in the Test Plan.	
	8.3	Unless otherwise agreed between the Parties, the Authority and the Contractor shall only commence each Test Stage and Test when all relevant agreed Entry Criteria for that Test Stage or Test have been met.	
	8.4	A Test Stage shall be recorded as successful if the number of errors unresolved at the end of the relevant Test Stage period does not exceed the agreed Error Thresholds and/or the acceptance criteria has been met for that Test Stage. The Contractor shall, within 3 Working Days of completion of a Test Stage, provide a summary report to the Authority providing such assurance as the Authority may reasonably require to demonstrate that the Entry and Exit Criteria for that stage have been satisfied.	
	8.5	If, after undertaking all applicable Tests but before a Test Stage was planned to finish, the number of unresolved errors is below the agreed Error Threshold, the Authority may, after consulting with the Contractor, notify the Contractor in writing that the Test Stage shall be successfully concluded at that point.	
	8.6	Unless otherwise agreed between the Parties, for any Test, a condition of commencing a Test Stage shall be that any and all preceding Test Stages for the Deliverables were also successful (unless otherwise agreed with the Authority Test Manager), including that the number of unresolved errors did not exceed the agreed Error Thresholds and/or acceptance criteria have been met for any and all preceding Test Stages.	
	8.7	Where errors remain unresolved at the end of any Test Stage period, but the agreed Error Threshold for that Test Stage has not been exceeded, such errors shall carry forward into the next Test Stage and if still unresolved count towards the Error Thresholds in that next Test Stage. The Authority reserves the right, acting reasonably, to delay the	

		commencement of subsequent test phases where it believes an unresolved Error could impact additional test phases.	
TEST ISSUES AND ERROR THRESHOLDS	9.1	Prior to the commencement of a Test Stage, and subject to paragraph 15.4, the Authority shall propose the Severity Level 3, Severity Level 4 and Severity Level 5 Error Thresholds for that Test Stage for agreement by the Contractor, which shall not be unreasonably withheld or delayed.	TEST ISSUES AND ERROR THRESHOLDS
	9.2	The Contractor's Test co-ordinator shall document all errors and Test Issues encountered during the Test in the Defect Management System and provide an update to the Authority on a daily basis, or as otherwise agreed, throughout the testing period. The Contractor's Test co-ordinator shall categorise each error as one of the following: (a) **Severity Level 1 Issue**: Critical Impact on business processes; fix required prior to Release; (i) a Test Issue that causes non-recoverable conditions, for example, it is not possible to continue using a component, a component crashes, there is database or file corruption, or data loss; (b) **Severity Level 2 Issue**: Major Impact on business processes; fix required prior to Release; (i) a Test Issue for which, as reasonably determined by the Authority, there is no practicable workaround available, and which: (A) causes a component to become unusable; (B) causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or (C) has an adverse impact on any other component(s) or any other area of the Services; (c) **Severity Level 3 Issue**: Minor Impact on business processes; fix preferred prior to Release; (i) a Test Issue which: (A) causes a component to become unusable; (B) causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or (C) has an impact on any other component(s) or any other area of the Services; but for which, as reasonably determined by the Authority, there is a practicable workaround available;	

		(d) **Severity Level 4 Issue**: Minor Impact on business processes; fix can be deferred until after Release; (i) a Test Issue which causes incorrect functionality of a component or process, but for which there is a simple, component based, workaround, and which has no impact on the current Test, or other areas of the Services; (e) **Severity Level 5 Issue**: Little Impact on business processes; fix can be deferred until after Release. (i) a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services.	
	9.3	The Contractor shall ensure that the Error Thresholds proposed for each Test Stage shall be no greater than: (a) no Severity Level 1 Issues; (b) no Severity Level 2 Issues; (c) 2 Severity Level 3 Issues; (d) 3 Severity Level 4 issues; and (e) 5 Severity Level 5 issues.	
	9.4	The Contractor shall be responsible for maintaining the Defect Management System and for ensuring that its contents accurately represent the current status of each Defect and Test Issue at all relevant times. The Contractor shall make the Defect Management System available to the Authority as per the requirement in Schedule 8.2 (Change).	Schedule 4.1 Organisation and Governance Section: 7.13 Test Tooling Paragraph: 7.13.4
	9.5	The Contractor's Test co-ordinator shall analyse and attempt to resolve each error in accordance with the incident tracking and management procedures agreed between the Parties.	Schedule 4.1 Organisation and Governance Section: 7.14 Testing: Defect Management
	9.6	The Contractor shall chair the joint meetings between the Contractor and Authority on a daily basis, or as otherwise agreed by the Authority, throughout each Test phase.	
TEST REPORT	10.1	Within 5 Working Days of completion of Testing of Deliverables, the Contractor will provide the Authority with a draft Test Report to the Authority. The Authority shall provide any comments on the draft Test Report no later than 5 Working Days after its receipt thereof.	Schedule 4.1 Organisation and Governance Section: 7.11 Testing: Planning and Execution Paragraph: 7.11.6
	10.2	On completion of the Testing of Deliverables the Contractor will provide the Authority with a finalised Test Report no later than fifteen (15)	

		Working Days after completion, taking into account any reasonable comments made by the Authority on the draft thereof in accordance with paragraph 10.1 above. Each Test Report (both the draft and final versions) shall provide a full report on the Testing conducted in respect of the relevant Deliverable, including: (a) an overview of the Testing conducted; (b) identification of the relevant Test Success Criteria that have been satisfied; (c) identification of the relevant Test Success Criteria that have not been satisfied, together with the Contractor's explanation of why those criteria have not been met, including any mitigations where necessary; (d) the Tests that were not completed together with the Contractor's explanation of why those Tests were not completed; and (e) the specification for any hardware and software used throughout the Testing of the relevant Deliverables and any changes that were applied to that hardware and/or software during the Testing. (f) a list of unresolved Testing errors/Defects, agreed by the Authority, that will be managed by the Problem Management process once Testing has been completed, as detailed in Schedule 2.1, Part 13 (IT Service Management).	
DEFECT REVIEW BOARD	11.1	The Contractor shall implement and maintain a working group comprising 2 members of the Contractor's personnel and 2 subject matter experts from the Authority (the "Defects Review Board"), whose purpose shall be to monitor and report on all Defects, errors and issues raised in the Defect Management System in accordance with the following timescales: (a) 30 days prior to the Operational Service Commencement Date, provide draft terms of reference for the Defect Review Board (the "Terms of Reference") for the Authority's review and approval (with the Authority providing any comments on the terms of reference within 10 days of receipt thereof; (b) 20 days prior to Operational Service Commencement Date and taking into account any reasonable comments made by the Authority on the Terms of References, finalise these terms; and (c) from the Operational Service Commencement Date and for the remainder of the Term, the Defect Review Board will come into effect and meet no less frequently than fortnightly or such other frequency as the Parties may agree;	Schedule 4.1 Organisation and Governance Section: 7.14 Testing: Defect Management Paragraph: 7.14.1

	11.2	The Contractor shall provide ongoing administrative support to the Defect Review Board and ensure pre-meeting materials are distributed no later than 2 Working Days prior to any meeting of the Defect Review Board, and that records of discussion are recorded and distributed to all attendees within 2 Working Days of any meeting being held.	
TEST SUCCESS OR TEST FAILURE	12.1	Following a Test, in accordance with the Testing Procedures and the applicable Test Plan, if all applicable Test Success Criteria are met, the Authority shall promptly issue to the Contractor a Test Certificate.	
	12.2	Following a Test, in accordance with the Testing Procedures and the applicable Product Test Plan, if all applicable Test Success Criteria are not met, the Authority shall promptly notify the Contractor of Test Failure and the reasons for such Test Failure.	
	12.3	Where there is a Test Failure, the Authority shall extend the Test Plan by such reasonable period or periods as the Authority may reasonably determine (provided that such extension does not result nor is likely to result in the failure (in whole or in part) of the Contractor meeting any Milestone or Key Milestone during the period in which the Contractor corrects the errors which caused the Test Failure and the Testing Procedures shall also be re-performed). To the extent the Test Failure is caused by the Contractor or any Contractor Personnel, all reasonable Authority costs incurred (arising out of further review or re-testing), as a direct result of such failure, relating to travel, expenses and resources, both internal and external, shall be paid in full by the Contractor once the Authority has provided receipts of the same to the extent possible.	
	12.4	If a Test Failure (or any proposed extension to the Test Plan following such Test Failure) results in or is likely to result in the failure (in whole or in part) by the Contractor to meet any Milestone or Key Milestone, then without prejudice to the Authority's other rights and remedies particularly as set out in Clauses 6 and 32 of this Agreement, the Contractor upon request by the Authority shall re-submit the relevant Deliverable for Testing and Clause 32 (Rectification Plan Process) in relation to the Authority's costs shall apply.	
	12.5	Subject to paragraph 12.3, the Authority and the Contractor shall each bear their own costs in respect of any Testing Procedures.	
ISSUE OF MILESTONE ACHIEVEMENT CERTIFICATE	13.1	The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following: (a) the issuing by the Authority of all Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that	

		Milestone which are due to be Tested; and performance by the Contractor to the reasonable satisfaction of the Authority of any other Milestone Achievement Criteria or other tasks identified in the Transition Plan and the Transformation Plan as associated with that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).	
	13.2	The grant of a Milestone Achievement Certificate shall entitle the Contractor to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 7.1 (Charges and Invoicing).	
	13.3	If there are Test Issues that do not exceed the Error Thresholds for the relevant Stage set out in paragraph 9.3 above, the Authority shall not be compelled to issue a Milestone Achievement Certificate but may elect, acting entirely at its own discretion, to issue a conditional Milestone Achievement Certificate which shall be conditional on the remediation of the relevant Test Issues in accordance with a rectification plan to be agreed between the Parties. The Contractor's entitlement to payment in accordance with paragraph 13.2 above shall be conditional on the completion of the remedial actions set out in the rectification plan.	
ITSM Maturity Assessments	13.4	The Authority shall not be required to issue any Milestone Achievement Certificate in respect of any Key Milestone within any Service Tower if the most recent ITSM Maturity Assessment was performed more than three months prior to the Milestone Date for a Key Milestone. If the most recent ISTM Maturity Assessment was performed more than 3 months prior to the Milestone Date for any Key Milestone, the Contractor may, with the Authority's prior consent: (a) adjust the projected date of the ITSM Maturity Assessment; or (b) procure a new ITSM Maturity Assessment, in each case so as to ensure that the most recent ITSM Maturity Assessment as at the date of the Milestone Achievement Certificate is no more than 3 months old	
	13.5	The Contractor shall complete the ITSM Maturity Assessments in accordance with paragraph 2.2 of Part 13 (IT Service Management) of Schedule 2.1 (Services Description) and shall complete: (a) the first ITSM Maturity Assessment no later the date falling two months after the Operational Service Commencement Date; and (b) the second ITSM Maturity Assessment no later than the date falling twelve months after the Operational Service Commencement Date.	

		Thereafter, the Contractor shall continue, for the remainder of the Term, to complete the ITSM Maturity Assessments on an annual basis, on or around the anniversary date of the Operational Service Commencement Date.	
Schedule 8.1 (Governance)			
MANAGEMENT OF THE SERVICES	1.1	The Contractor and the Authority shall each appoint an appropriate authorised senior representative for the purposes of this Agreement through whom the Services shall be managed at a day-to-day.	Schedule 4.1 Organisation and Governance Section: 1 Organisation Paragraph: 2.1.1
	1.2	Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Agreement can be fully realised.	Schedule 4.1 Organisation and Governance Section: 1 Organisation Paragraph: 2.2.2
	1.3	Governance Structure	
RELATIONSHIP MANAGEMENT PLAN	2.1	The Relationship Management Plan is set out in Appendix 3.	
	2.2	The Contractor shall submit a draft of the Detailed Relationship Management Plan to the Authority for approval within 10 Working Days of the Effective Date.	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.3
	2.3	The Contractor shall ensure that the draft Detailed Relationship Management Plan sets out how the Parties will work together during the Term and includes detail relating to: (a) the identity of the nominated Relationship Manager; (b) how the Contractor will interact with the Authority and deal with any Authority feedback; (c) how the Parties will behave reasonably in dealing with one another including in relation to the activities in table 1 below; (d) how the Parties will cooperate with respect to principles regarding: (i) openness and honesty, and engaging with stakeholders; (ii) mutual respect and valuing each individual's contribution; (iii) encouraging innovation and continuous improvement; (iv) solving problems quickly in a non-confrontational, no-blame manner; (v) being flexible and cost conscious in response to change; (vi) adopting best practice and managing risk;	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.3 - 2.14.4

		(vii) providing safe working conditions; (viii) respecting and protecting the environment; and (ix) making work as enjoyable as possible.	
	2.4	Following receipt of the draft Detailed Relationship Management Plan from the Contractor, the Authority shall: (e) review and comment on the draft Detailed Relationship Management Plan as soon as reasonably practicable; and (f) notify the Contractor in writing that it approves or rejects the draft Detailed Relationship Management Plan no later than 10 Working Days after the date on which the draft Detailed Relationship Management Plan is first delivered to the Authority.	
	2.5	If the Authority rejects the draft Detailed Relationship Management Plan: (g) the Authority shall inform the Contractor in writing of its reasons for its rejection; and (h) the Contractor shall then revise the draft Detailed Relationship Management Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Relationship Management Plan to the Authority for the Authority's approval within 5 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 2.4 and this Paragraph 2.5 shall apply again to any resubmitted draft Detailed Relationship Management Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.6
	2.6	If the Authority approves the draft Detailed Relationship Management Plan, it shall replace the Outline Relationship Management Plan from the date of the Authority’s notice of approval.	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.7
	2.7	The Parties will keep under review the processes and mechanisms for building and maintaining their relationship in line with the principles set out in this paragraph and as set out in the Relationship Management Plan.	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.8
	2.8	In relation to the Boards and Fora set out in this Schedule 8.1 the Parties will adhere to the Principles set out in the Relationship Management Plan.	Schedule 4.1 Organisation and Governance Section: 2.14 Relationship Management And Collaboration Paragraph: 2.14.9

BOARDS Establishment and structure of the Boards	3.1	The Boards shall be established by the Authority for the purposes of this Agreement on which both the Contractor and the Authority shall be represented.	
	3.2	Both Parties shall ensure appropriately qualified, experienced and empowered personnel attend meetings as agreed between the Authority and the Contractor.	Schedule 4.1 Organisation and Governance Section: 1 Organisation Paragraph: 2.1.2
	3.3	In relation to each Board, the: (a) Authority Board Members; (b) Contractor Board Members; (c) frequency that the Board shall meet (unless otherwise agreed between the Parties); (d) location of the Board's meetings; and (e) planned start date by which the Board shall be established, shall be as set out in Appendix 1.	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.2.3
	3.4	In the event that either Party wishes to replace any of its appointed Board Members, that Party shall notify the other in writing of the proposed change for agreement by the other Party (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority Board Member has at all times a counterpart Contractor Board Member of equivalent seniority and expertise.	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.2.4
Board meetings	3.5	Each Party shall ensure that its Board Members shall make all reasonable efforts to attend Board meetings at which that Board Member's attendance is required. If any Board Member is not able to attend a Board meeting, that person shall use all reasonable endeavours to ensure that: (a) a delegate attends the relevant Board meeting in his/her place who (wherever possible) is properly briefed and prepared; and (b) that he/she is debriefed by such delegate after the Board Meeting.	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.3.1 - 2.3.3
	3.6	A chairperson shall be appointed by the Authority for each Board as identified in Appendix 1. The chairperson shall be responsible for: (a) scheduling Board meetings; (b) setting the agenda for Board meetings and circulating to all attendees in advance of such meeting; (c) chairing the Board meetings; (d) monitoring the progress of any follow up tasks and activities agreed to be carried out following Board meetings;	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.3.4

		(e) ensuring that minutes for Board meetings are recorded and disseminated electronically to the appropriate persons and to all Board meeting participants within seven Working Days after the Board meeting; and (f) facilitating the process or procedure by which any decision agreed at any Board meeting is given effect in the appropriate manner.	
	3.7	Board meetings shall be quorate as long as at least two representatives from each Party are present.	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.3.5
	3.8	The Parties shall ensure, as far as reasonably practicable, that all Boards shall as soon as reasonably practicable resolve the issues and achieve the objectives placed before them. Each Party shall endeavour to ensure that Board Members are empowered to make relevant decisions or have access to empowered individuals for decisions to be made to achieve this.	Schedule 4.1 Organisation and Governance Section: 2.2 Boards Paragraph: 2.3.6
ROLE OF THE PORTFOLIO MANAGEMENT BOARD	4.1	The Portfolio Management Board shall: (a) provide senior level guidance, leadership and strategy for the overall delivery of the Transformation Plan and through life change.; (b) be the point of escalation from the Joint Change Advisory Board, the Joint Architecture Governance Board, the Transition Management Board and the Transformation Management Board ; and (c) carry out the specific obligations attributed to it in Paragraph .2.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority
	4.2	The Portfolio Management Board shall: (a) ensure that this Agreement is operated throughout the Term in a manner which optimises the value for money and operational benefit derived by the Authority and the commercial benefit derived by the Contractor; (b) receive and review reports from the Service Review Board or appropriate and review reports on technology, service and other developments that offer potential for improving the benefit that either Party is receiving, in particular value for money; (c) determine business strategy and provide guidance on policy matters which may]#impact on the implementation of the Services or on any Optional Services; and	

		(d) authorise the commissioning and initiation of, and assess opportunities for, Optional Services; and (e) provide guidance and authorisation to the Joint Change Advisory Board on relevant Changes.	
ROLE OF THE SERVICE REVIEW BOARD	5.1	The Service Review Board shall be responsible for the executive management of the Services and shall: (a) be accountable to the DBS Operations Board for comprehensive oversight of the Services and for the senior management of the operational relationship between the Parties; (b) report to the DBS Operations Board on significant issues requiring decision and resolution by DBS Operations Board and on progress against the Transition Plan (including the progress of Transferring WIP); (c) receive reports on matters such as issues relating to delivery of existing Services and performance against Performance Indicators, progress against the Transition Plan (including the progress of Transferring WIP), and those elements of the Transformation Plan which will impact Service delivery and any other future developments; (d) review and report to the Portfolio Management Board on service management, co-ordination of individual projects and any integration issues; (e) deal with the prioritisation of resources which impact Service delivery on behalf of the Parties; (f) consider and resolve Disputes (including Disputes as to the cause of a Delay or the performance of the Services) in the first instance and if necessary escalate the Dispute to the DBS Operations Board ; (g) develop operational/Contractor relationship and develop and propose the relationship development strategy and ensure the implementation of the same; (h) consider input from the Service Delivery Working Group, Transition Management Board and Relationship Management Forum as detailed in Appendix 2; and (i) review and report on joint risks impacting Service delivery and agree the Crown Commercial Services performance monthly report. (j) review a rolling 18 month forward programme of Service delivery activity, including, anticipated changes in demand (volume and/or scope),	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority

		new initiatives or legislation, or changes to sites from which Services are delivered	
ROLE OF THE JOINT CHANGE ADVISORY BOARD	6.1	The JCAB shall be a joint review board consisting of nominated representatives from both Authority and Contractor staff, the involvement of which will be determined by the Change subject or Deliverable to ensure that the Change Requests are thoroughly checked and assessed from both a technical and business perspective.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority Section: 7.4 The Joint Change Advisory Board (JCAB)
	6.2	Where the Contractor disagrees with the Authority regarding the classification or category of a Change, this will be minuted by the JCAB, outlining the reasons and/or any mitigations. Where an agreement cannot be established within a further ten Working Days, the provisions of Schedule 8.3 (Dispute Resolution Procedure) shall apply.	
	6.3	Where the Contractor requires more information from the Authority in order to classify, categorise or approve a Change Request, the Contractor shall submit a request for clarification to the Authority within five Working Days of receipt of the Change Request.	
	6.4	Either Party may call an emergency JCAB ("e-JCAB") meeting to discuss and approve Emergency Change Requests as and when required.	
	6.5	The Joint Change Advisory Board shall assess the impact and approve or reject all Change Requests. Changes which will have a significant impact on the Services shall be escalated to the Portfolio Management Board.	
	6.6	The Joint Change Advisory Board shall: (a) review Change Requests; (b) analyse and record the impact of all Changes, specifically whether the proposed Change: (i) has an impact on other areas or aspects of this Agreement and/or other documentation relating to the Services; (ii) has an impact on the ability of the Authority to meet its agreed business needs within agreed time-scales; (iii) will raise any risks or issues relating to the proposed Change; and (iv) will provide value for money in consideration of any changes to the Financial Model, future Charges and/or Performance Indicators and Target Performance Levels; (c) provide recommendations, seek guidance and authorisation from the Portfolio Management Board as required; and	

		(d) approve or reject (close) all proposed Changes Change Requests within five Working Days of receipt (being raised on the Change Management System).	
	6.7	The Contractor shall provide suitably qualified and experienced personnel at all JCAB meetings to enable all Change Requests to be reviewed and assessed to determine: (a) the validity of the request; (b) the category of change (in accordance with Appendix 1 to Schedule 8.2 (Change Control Procedure)); (c) the priority; and (d) the delivery methodology (e.g. Agile, Waterfall or hybrid).	
ROLE OF THE JOINT ARCHITECTURE GOVERNANCE BOARD	7.1	The Joint Architecture Governance Board cture Board) shall be accountable to the Portfolio Management Board for oversight of the technology used in the Contractor Solution and ensuring that technological choices are made to maximise the long term value of the Contractor Solution as a business asset of the Authority.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority
	7.2	The Joint Architecture Governance Board shall: (a) ensure compliance with the Standards; (b) grant dispensations for variations from such compliance where appropriate; (c) assure the coherence and consistency of the systems architecture for the Contractor Solution; (d) monitor developments in new technology and reporting on their potential benefit to the Services; (e) provide advice, guidance and information on technical issues; (f) assure that the technical architecture of the Contractor Solution is aligned to the Service Requirements and has sufficient flexibility to cope with future requirements of the Authority; and (g) where necessary escalate any issues to the Portfolio Management Board,	
TRANSFORMATION MANAGEMENT BOARD	8.1	The Transformation Management Board shall develop, coordinate and manage transformation activity across the Future Services Delivery Contract (FSDC) and ensure that service improvements and savings are delivered in line with the Contractor's Transformation Plan and milestone regime and is accountable to the Portfolio Management Board.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority
	8.2	The Transformation Management Board shall escalate issues that may impact the delivery of the Transformation Plan to the Portfolio Management Board.	

	8.3	The Transformation Management Board shall: (a) provide the overarching governance and decision making framework for the Contractor's Transformation Plan; (b) agree the overall programme goals, objectives and priorities; (c) reviews will include rapid improvement interventions, lean systems reviews, structural reviews and fundamental service reviews; (d) monitor and manage programme progress, savings and impact; (e) provide a robust challenge and scrutiny function for all reviews; (f) manage high-level interdependency's and risks associated with all transformation programmes and the wider portfolio of change; (g) strategically identify, prioritise and allocate resources to programmes and projects, re-aligning where necessary; (h) identify and develop funding and resource plans designed to assist in the delivery of the programme; (i) ensure transformation milestones deliver against agreed outcomes, KPI's, budgets, timescales and business benefits; (j) monitor and approve Milestone Achievement Certificates, if all Milestone Achievement Criteria have been met; (k) put in place an over-arching effective communications and engagement strategy, sharing key messages with employees, members and partners as required; (l) ensure that programme leads are adequately supported in their work and held to account for the delivery of their responsibilities; (m) receive reports on matter such as issues relating to existing services which may impact on elements of the Transformation Plan.	
TRANSITION MANAGEMENT BOARD	9.1	Not less than 10 Working Days after the Effective Date the Parties shall establish a Transition Management Board which shall include appropriate representatives from the Authority, the Contractor and the relevant Outgoing Contractors.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority
	9.2	The Transition Management Board shall be accountable to the Service Review t Board;	
	9.3	The scope of transition shall include but not be limited to transition project governance, people management, transfer of operational responsibilities and services, security readiness, governance process readiness and technology readiness,	
	9.4	The Transition Management Board shall meet on a regular basis to: (a) review the Transition Plan;	

		(b) oversee progress against the overall Transition Milestones Regime and Achievement Criteria; (c) asses and manage any risks and issues relating to the Transition Milestone Regimes and where necessary escalate any issues to the Service Review Board; (d) identify the WIP by the outgoing contractor(s) and the potential Transferring WIP; (e) take steps to ensure that as much WIP as possible is cancelled if no longer required or completed prior to the relevant WIP Transfer Date and refine the scope of the potential Transferring WIP; (f) prior to the WIP Transfer Date, agree the steps required for the Contractor to assume responsibility for the completion of the Transferring WIP from the WIP Transfer Date; (d) prior to the WIP Transfer Date, document and agree (the Parties acting reasonably) the Transferring WIP and its categorisation as Operational Services (which shall constitute the agreed Transferring WIP). Transferring WIP shall be completed, unless agreed otherwise, as a Operational Service where the relevant work would be designated as a Operational Service under this Agreement;	
RELATIONSHIP MANAGEMENT FORUM	10.1	The purpose of the Relation Management Forum is to provide an environment to review, the efficacy and effectiveness of the Relationship Management Plan.	Schedule 4.1 Organisation and Governance Section: 2.12 Interfaces with the Authority
	10.2	The Relationship Management Forum shall: (a) Review and develop in an open and constructive way: (i) issues (ii) processes (iii) behaviours. Concerning the relationship at all levels (b) remain up-to-date on emerging issues; (c) promote partnering behaviours.	
	10.3	The Relationship Management Forum shall be accountable to the Service Review Board.	
	10.4	The Relationship Management Forum terms of reference will be reviewed on an annual basis.	
	10.5	Sub groups may be convened where necessary.	
	10.6	The Contractor Relationship Manager and the Authority Relationship Manager will present a joint report to the Relationship Management	

		Forum at each meeting. This report will include results of actions previously taken by the Relationship Management Forum.	
	10.7	The outcomes from each meeting will be a record of decisions and an overall summary.	
	10.8	Meetings will be organised and agreed by the Contractor Relationship Manager and the Authority Relationship Manager.	
	10.9	The Agenda will be drafted and agreed by the Contractor Relationship Manager and the Authority Relationship Manager.	
	10.10	Any evidence or papers for consideration will be circulated at least 5 working days in advance to all attendees.	
OPERATIONAL GROUPS MEETINGS	11.1	In addition to the Boards, the Authority will establish the Groups set out in Appendix 2 below	Schedule 4.1 Organisation and Governance Section: 2.9 Effective tools and techniques for Relationship Management Plan Paragraph: 2.9.1
	11.2	Both Parties shall ensure appropriately qualified, experienced and empowered personnel attend meetings as agreed between the Authority and the Contractor.	
	11.3	In relation to each Group, the: (a) Authority Board Members; (b) Contractor Board Members; (c) frequency that the Group shall meet (unless otherwise agreed between the Parties); (d) location of the Group's meetings; and (e) planned start date by which the Group shall be established, shall be as set out in Appendix 2.	
CONTRACT MANAGEMENT MECHANISMS	12.1	Both Parties shall pro-actively manage risks attributed to them under the terms of this Agreement.	Schedule 4.1 Organisation and Governance Section: 3 Risk Management Overview & Organisation
	12.2	The Contractor shall develop, operate, maintain and amend, as agreed with the Authority, processes for: (a) the identification and management of risks; (b) the identification and management of issues; and (c) monitoring and controlling project plans.	
	12.3	The Risk Register shall be updated by the Contractor and submitted for review by the Service Review Board.	

ANNUAL REVIEW	13.1	An annual review meeting shall be held throughout the Term on a date to be agreed between the Parties.	Schedule 4.1 Organisation and Governance Section: 2.5 Annual Review
	13.2	The meetings shall be attended by the [insert role] of the Contractor and the [insert role] of the Authority and any other persons considered by the Authority necessary for the review.	
Schedule 8.2 (Change Control Procedure)			
INTRODUCTION	1	This Schedule sets out the procedure for dealing with Changes.	
CHANGE REQUIREMENTS	2.1	In addition to the Change Control Procedures set out in this Schedule, the Contractor shall comply with Paragraph 5.5 (Change Management System) of Appendix 1 of Part 13, Annex M to Schedule 2.1 (Service Requirements - Information Technology Service Management) in relation to: (a) developing and maintaining a workflow based automated Change Management System; and (b) the planning and management of change related to IT Service Management.	Schedule 4.1 Organisation and Governance Section: 1.2 Change Management
	2.2	Whether a Change is an Operational Change or a Contract Change, all Changes shall be logged and processed through the Change Management System. The Parties may agree in the Service Operations Manual those categories of business as usual Operational Change which are exempt from the Change Management System.	Schedule 4.1 Organisation and Governance Section: 2.6 Change Management Paragraph: 2.6.3
	2.3	To the extent that any Change Request relates to the Contractor System the Parties shall also follow: (a) the procedures set out in Schedule 6.2 (Testing Procedures); and (b) the change requirements in Paragraph 5 (Service Change) of Appendix 1 of Part 13, Annex M to Schedule 2.1 (Service Description – Technical).	Schedule 4.1 Organisation and Governance Section: 2.7 Change Management Paragraph: 2.6.1
Requirements Development	2.4	Where reasonably requested by the Authority, Contractor Personnel shall support and assist the Authority with the discovery, identification, and agreement of Change requirements. Such support activities shall include but are not limited to: (a) analysis of statements of business capability and associated requirements to establish whether they are necessary and sufficient; (b) analysis of requirements to balance the Authority's stakeholder needs and constraints;	Schedule 4.1 Organisation and Governance Section: 7.1 Introduction and Requirements Definition Support

		(c) validation of requirements to ensure resulting products and services shall perform as intended in terms of meeting stated business capabilities and operating in the Authority's ICT environment; and (d) attendance at change development meetings and/or workshops.	
CLASSIFICATION OF CHANGE	3.1	A Change may either be: (a) an Operational Change, which shall be processed in accordance with Paragraphs 4 (Change Requests) and 5 (Operational Change Procedure); or (b) a Contract Change, which shall be processed in accordance with Paragraphs 4 (Change Requests), 6 (Contract Change Procedure), and 7 (Impact Assessment).	Schedule 4.1 Organisation and Governance Section: 7.2 Change Administration Tooling and Reporting Paragraph: 7.2.2
CHANGE REQUESTS	4.1	All Changes must be requested via the Change Request form. The final form of the Change Request form shall be agreed by the Parties 30 calendar days prior to Operational Services Commencement Date. The Parties may agree in the Service Operations Manual those categories of business as usual Operational Change which are exempt from the Change Management System.	Schedule 4.1 Organisation and Governance Section: 7.5 Change Administration Tooling and Reporting
	4.2	All new and outstanding Change Requests shall be reviewed by the JCAB on a weekly basis (or more frequently if so requested to by the Authority) who shall categorise each Change Request in accordance with the Change Categories in Appendix 1 (Categories of Change).	
	4.3	Ahead of each JCAB meeting, the Contractor shall distribute to the Authority: (a) no later than 1 Working Day prior to the JCAB meeting, all relevant documents to support the delivery of the JCAB meeting (including but not limited to the agenda, new and outstanding Change Requests and any supporting documentation); (b) no later than 2 Working Days following the JCAB meeting, the records of decisions made and actions to be taken as agreed during the JCAB meeting; and (c) the Contractor shall provide all administration support for the JCAB.	
	4.4	The Authority shall have the right to request amendments to a Change Request, approve it, or reject it in the manner set out in Paragraph 10.1 (Authority's right of Approval).	
	4.5	The Contractor shall have the right to reject a Change Request solely in the manner set out in Paragraph 10.2 (Contractor's right of Approval).	

	4.6	If the Contractor requires any clarification on a Change Request, the Contractor shall promptly submit a request for clarification to the Authority and the Authority shall respond to such request for clarification as soon as reasonably practicable. Provided that sufficient information is received by the Authority on the nature of the request for clarification and the Contractor has provided a reasonable justification for the request, the Authority may at its sole discretion, acting reasonably, extend the time period by such reasonable period of time (as agreed between the Parties) for the Contractor to complete the Impact Assessment (if applicable).	
OPERATIONAL CHANGE PROCEDURE	5.1	Subject to Paragraph 5.3, either Party may request an Operational Change by submitting a Change Request to the Contractor Change Manager which shall include the following details: (a) the proposed Operational Change; (b) the timescale for completing the Operational Change which shall be: (i) where applicable, as specified in relevant Service Requirement; (ii) calculated in accordance with the timescales set out in Appendix 1 (Categories of Change); or (iii) such other timescale as may be agreed by the Authority acting reasonably; and (c) whether the proposed Operational Change is within the scope of the Service Catalogue;	Schedule 4.1 Organisation and Governance Section: 7.5 Change Administration Tooling and Reporting
	5.2	Where the proposed Operational Change is not included in the Service Catalogue once a Change Request has been approved, the Contractor shall provide an Impact Assessment and, if required by the Authority, the Contractor shall add the detail of that Change, including the relevant Impact Assessment, to the Service Catalogue for subsequent reference.	
	5.3	Where the proposed Operational Change relates to Transformation the deployment of that Change will require an Impact Assessment and the Change will be processed in accordance with the Detailed Transformation Plan requirements set out in Schedule 6.1 (Transition and Transformation Plans).	
	5.4	Subject to approval of: (a) the Change Request by the JCAB; and (b) where applicable, the Impact Assessment by the Authority,	

		the Contractor shall implement the Operational Change within the timescale specified for completion of the Operational Change in the approved Change Request.	
	5.5	Following completion of the Operational Change, the Contractor shall promptly notify the Authority and provide the Authority with details of completion of the relevant Operational Change.	
	5.6	The Contractor shall not be entitled to increase the Charges in respect of Operational Changes.	
CONTRACT CHANGE PROCEDURE	6.1	Either Party may request a Contract Change.	Schedule 4.1 Organisation and Governance Section: 7.5 Change Administration Tooling and Reporting
	6.2	For Change Requests raised for a Contract Change, the Change Request shall state whether the Party issuing the Change Request considers the proposed Change will include a Gain Share Opportunity arising from the Contractors obligations under Clause 8 (Services Improvement).	
	6.3	Save as otherwise provided in this Schedule, the Contractor shall assess and document the potential impact of a proposed Contract Change in accordance with Paragraph 7 (Impact Assessment).	
	6.4	Save as otherwise provided in this Schedule, no proposed Contract Change shall be implemented by the Contractor until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 10.1(b) (Authority's right of Approval).	
	6.5	The Parties acknowledge that there may be circumstances where it is necessary for the Contractor to start development work ahead of a Change Authorisation Note being issued by the Authority. In these circumstances the Parties may agree to implement the Fast Track procedure in accordance with Paragraph 8 (Fast Track Procedure).	
	6.6	To the extent that any Contract Change requires testing and/or a programme for implementation, where appropriate, the Change Authorisation Note relating to such a Contract Change shall specify Milestones and/or a Key Milestone and Milestone Date(s) in respect of such Contract Change for the purposes of such procedures.	
	6.7	Until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 10.1(b) (Authority's right of Approval), then:	

		(a) unless the Authority expressly agrees (or requires) otherwise in writing, the Contractor shall continue to supply the Services in accordance with the existing terms of this Agreement as if the proposed Contract Change did not apply; and (b) any discussions, negotiations or other communications which may take place between the Authority and the Contractor in connection with any proposed Contract Change, including the submission of any Impact Assessment or other supporting documents, shall be without prejudice to each Party's other rights under this Agreement.	
	6.8	At the end of each calendar Month the Contractor shall deliver to the Authority a copy of this Agreement updated to reflect all Contract Changes agreed during the preceding calendar month annotated with reference to each relevant Change Authorisation Note pursuant to which the relevant Contract Changes were agreed.	
IMPACT ASSESSMENT	7.1	The Contractor shall provide an Impact Assessment in response to all Changes, within the timelines set out in Appendix 1 (Categories of Change).	Schedule 4.1 Organisation and Governance Section: 7.5 Change Initiation, Impact and Approval/Rejection Paragraph: 7.5.4 - 7.5.5
	7.2	All proposals which would, if accepted, have an impact on the Charges must be transparent, contain an appropriate level of detail to facilitate scrutiny and assessment of Value for Money, and be proportionate to the type of Change under consideration.	
	7.3	Where a Contractor's proposal includes a reduction in the Charges, or where the Authority reasonably believes there should be a reduction in the Charges, the Contractor shall evidence how it will achieve a reduction in the Charges by supplying: (a) an analysis of the cost reductions that shall be achieved as a result of the proposed Change (supported by relevant documentary evidence of the reduction) and any other information reasonably requested by the Authority in connection with the reduction; or (b) where the proposal does not evidence a reduction in the Charges or where the Authority reasonably believes the proposal does not adequately evidence a reduction in the Charges, written justification together with documentary evidence demonstrating why the Contractor is unable to make the requested reduction in the Charges.	
	7.4	Any project and programme management costs shall not exceed 20% of the total cost of the Change, unless agreed in writing by the Authority.	

		Subject to the Authority's right under Paragraph 10.1 (Authority's right of Approval) such agreement is not to be unreasonably withheld or delayed.	
	7.5	Each Impact Assessment shall include: (a) details of the proposed Change including the reason for the Change and benefits that will accrue to the Authority if the Change were implemented; (b) an assessment of the impact of the proposed Change on: (i) the Services and the Contractor's ability to meet its other obligations under this Agreement; (ii) any relevant external interfaces; (iii) the working practices of either Party; (iv) the risk profile of the Services and/or this Agreement; (v) the BCDR Plans and services; (vi) the key risks associated with the Change, including an assessment of their likelihood and impact, and actions taken to mitigate them; (vii) other services provided by either the Authority, or any Third Party Contractors (to the extent the Contractor has knowledge of such services); (viii) any Authority Responsibilities; and (ix) the Sub-contracting arrangements; (c) the proposed delivery methodology (Agile, Waterfall, hybrid) including a timetable for the implementation, together with: (i) details of documentary deliverables; (ii) any proposals for the Testing of the Change; (iii) recommendations of where the proposed Change should fit into the overall Forward Schedule of Change and any relevant Release Plan; (iv) the proposed roll-back, fall-back and recovery procedures (if any) which would apply if the implementation of the proposed Change fails in whole or in part; (v) details of any milestones and/or check points (including dates) in respect of such proposed Change; and (vi) any other matter reasonably requested by the Authority at the time of the Impact Assessment, or reasonably considered by the Contractor to be relevant; (d) where the Change Request relates to a Contract Change: (i) details of any proposed variation to the terms of this Agreement that will be required; and	

		(ii) details of the following costs, broken down into both Contract Year and Financial Year: (A) the cost of implementing the proposed Contract Change; (B) the ongoing costs (including the total cost of delivery and any future running costs) and any alteration to the working practices of either Party as a result of implementing the proposed Contract Change; (C) any increase or decrease in the Charges; (D) any Gain Share; (E) any alteration in the resources and/or expenditure required by either Party; and (F) any project and programme management costs; (e) where the Change Request relates to a Change directly to the Mil Pers & Vets Reporting Platform or to any system used as a data source by the platform, details of all existing reporting items (e.g. Analysis, Report, Dashboard, query) impacted must include, but not be limited to: (i) the name of the impacted item; (ii) the item owner; (iii) detail of the impact upon the item; (iv) the last execution date of the item; and (v) Impact mitigation recommendations; (f) details of how the proposed Change will ensure compliance with any applicable Change in Law; (g) written confirmation from the Guarantor that the proposed Change is within the scope of the Guarantee provided that to the extent that the Guarantee authorises such Change as being within its scope the Authority may waive this requirement; (h) if so requested by the Authority, a plan for the levels of resource needed to deliver the Change (including quantities of labour, equipment and materials); and (i) such other information as the Authority may reasonably request in (or in response to) the Change Request.	
	7.6	If the Contractor considers that a proposed Change has no risks or impact of the kind described in Paragraph 7.5, it shall include a written statement to that effect in the Impact Assessment	Schedule 4.1 Organisation and Governance Section: 7.5 Change Administration Tooling and Reporting Paragraph: 7.5.6

	7.7	Subject to the provisions of Paragraph 7.8, the Authority shall review the Impact Assessment and respond to the Contractor in accordance with Paragraph 8 (Fast Track Procedure) within 15 Working Days of receiving the Impact Assessment.	
	7.8	If the Change is raised by the Contractor, and the Authority reasonably considers that it requires further information regarding the proposed Change in order that it may evaluate the Change Request and the Impact Assessment, the Contractor shall provide the further information requested within 10 Working Days or such other period as may reasonably be agreed, and re-issue the relevant Impact Assessment where appropriate. At the Authority's discretion, the Parties may repeat the process described in this Paragraph 7.8 until the Authority is satisfied that it has sufficient information to evaluate the Change Request and Impact Assessment.	
	7.9	The calculation of any proposed price increase for the purposes of 7.3 and 7.5(d)(ii)(C) shall: (a) where applicable be based on the prices set out in the Service Catalogue and/or the Financial Model; (b) be consistent with the level of Contractor overhead and margin set out in the Financial Model; (c) facilitate the Financial Transparency Objectives; (d) demonstrate how the Contractor is ensuring value for money for the Authority; (e) include estimated volumes of each type of resource to be employed and the applicable Rate Card; (f) include full disclosure of any assumptions underlying such Impact Assessment; (g) include evidence of the cost of any assets required for the Change; and (h) include details of any new Sub-Contracts necessary to accomplish the Change.	
FAST TRACK PROCEDURE	8.1	The Parties acknowledge that to ensure operational efficiency, there may be circumstances where it is desirable to expedite the Contract Change Procedure.	Schedule 4.1 Organisation and Governance Section: 7.7 Fast-Track Change
	8.2	If the Contractor believes that the Contract Change Procedure will not allow the completion of the Contract Change within the necessary timescales, the Contractor may request to start development work for the	

		Contract Change under the Fast Track Procedure by submitting a Fast Track Request Form to the Authority's Commercial Officer.	
	8.3	The Authority may at its absolute discretion approve the Fast Track Request Form. If the Contractor commences delivery of the Change Request prior to approval of the Fast Track Request Form, it does so at its own risk.	
	8.4	Following approval of a Fast Track Request Form by the Authority's Commercial Officer, the Contractor shall: (a) commence delivery of the approved Contract Change; and (b) as soon as reasonably practicable and in any event no later than 10 Working Days, submit to the Authority its Impact Assessment in accordance with Paragraph 7 (Impact Assessment).	
	8.5	The Authority reserves the right to reject any Impact Assessment which is submitted under Paragraph 8.3 and to cancel the Change Request.	
	8.6	In the event that the Authority notifies the Contractor that it has cancelled a Change Request that has been commenced under the Fast Track Change Control Procedure, the Authority will only be liable for unrecoverable costs incurred by the Contractor to the date of Notice by the Authority that the Change Request is cancelled.	
	8.7	The Contractor shall not exceed the costs as detailed in the approved Fast Track Request Form. Where the Contractor anticipates that such agreed costs may be exceeded, it shall submit an additional Fast Track Request Form to the Authority's Commercial Manager for approval. Where the Contractor exceeds the costs specified in the agreed Fast Track Request Form, it does so at its own risk.	
EMERGENCY CHANGE	9.1	If any Change to the Contractor System has to be delivered by reason of urgency, or in an emergency, in order to keep the system safe (i.e. a security issue) or to, maintain business continuity then: (a) the Authority can authorise the Contractor to deliver the Change as an Emergency Change within such timelines as are agreed by the Parties and in any case no later than 2 Working Days; or (b) the Contractor may, acting reasonably, choose to deliver the Change as an Emergency Change and, within 24 hours, notify the Authority of such Emergency Change.	Schedule 4.1 Organisation and Governance Section: 7.16 Retrospective Change
	9.2	The Contractor shall employ a consistent way of working to ensure all Emergency Change is delivered in accordance with the Service Operations Manual.	

	9.3	Where Emergency Change is delivered out of normal working hours, all necessary documentation is to be retrospectively raised by the Contractor and approved by the JCAB within 5 Working Days.	
	9.4	Where Emergency Change is delivered, the Contractor shall deliver an Impact Assessment within the timescales agreed by Authority (Change Manager).	
	9.5	The Authority may (acting reasonably having regard to the nature of the emergency) choose to Test (including Witness Testing where appropriate in accordance with Schedule 6.2 (Testing Procedure)), any Emergency Change prior to the deployment of the Change.	
APPROVAL AND AMENDMENTS	10.1	**Authority's right of Approval** (a) Within 15 Working Days of receiving the Impact Assessment from the Contractor, or on receipt of the further information that it may request pursuant to Paragraph 7.8 (Impact Assessment), the Authority shall evaluate the Impact Assessment and shall do one of the following: (i) approve the proposed Impact Assessment, where the Parties shall follow the procedure set out in Paragraph 10.1(b); (ii) in its absolute discretion, reject the Impact Assessment, where the Authority shall notify the Contractor of the rejection. The Authority shall not reject any proposed Impact Assessment to the extent that the Change is necessary for the Contractor or the Services to comply with any Changes in Law. If the Authority does reject a Contract Change, then it shall explain its reasons in writing to the Contractor as soon as is reasonably practicable following such rejection; or (iii) in the event that the Authority reasonably believes that a Change Request or an Impact Assessment contains errors or omissions, require the Contractor to modify the relevant document within 5 Working Days of request. Subject to Paragraph 7.8, on receiving the modified Impact Assessment, the Authority shall approve or reject the proposed Impact Assessment within 15 Working Days. (b) If the Authority approves the proposed Impact Assessment pursuant to Paragraph 10.1(a)(i), and it has not been rejected by the Contractor in accordance with Paragraph 10.2)), the Authority shall inform the Contractor and the Contractor shall prepare two copies of a Change Authorisation Note, which it shall sign and	Schedule 4.1 Organisation and Governance Section: 7.5 Change Initiation, Impact and Approval/Rejection

		deliver to the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign both copies and return one copy to the Contractor. On the Authority's signature, the Change Authorisation Note shall constitute (or, where the Authority has agreed to or required the implementation of a Change prior to signature of a Change Authorisation Note, shall constitute confirmation of) a binding variation to this Agreement. (c) If the Authority does not sign the Change Authorisation Note within 10 Working Days, then the Contractor shall have the right to notify the Authority and if the Authority does not sign the Change Authorisation Note within 5 Working Days of such notification, then the Contractor may refer the matter to the Expedited Dispute Timetable pursuant to the Dispute Resolution Procedure.	
	7.2	**Contractor's right to reject** Following the delivery of an Impact Assessment, if: (a) the Contractor reasonably believes that any proposed Change which is requested by the Authority would: (i) materially and adversely affect risks to the health and safety of any person; and/or (ii) require the Services to be performed in a way that infringes any Law; and/or (b) the Contractor demonstrates to the Authority's reasonable satisfaction that the proposed Change is technically impossible to implement and neither the Contractor Solution nor the Services Description state that the Contractor does have the technical capacity and flexibility required to implement the proposed Contract Change, the Contractor shall be entitled to reject the proposed Change and shall notify the Authority of its reasons for doing so within 5 Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to Paragraph 7.1 (Impact Assessment).	
COST OF PREPARING CHANGE REQUEST	11.1	Subject to Paragraph 11.2: (a) the costs incurred by the Contractor in preparing a Change Request shall be borne by the Contractor; (b) where reasonably requested by the Authority, the Contractor shall provide functional and technical help, advice and support in defining requirements and preparing a Change Request for submission to the JCAB. Any costs incurred in providing this	

		service shall be borne by the Contractor, including but not limited to any costs associated with attendance at meetings and/or workshops; and (c) the costs incurred by the Contractor in undertaking an Impact Assessment shall be borne by the Contractor.	
	11.2	The Contractor shall: (a) provide documentary evidence to the Authority which demonstrates to the Authority's satisfaction that best value for money has been or will be achieved; and (b) provide such other information and assistance as the Authority reasonably requests in relation to any value for money assessment, and in establishing the Contractor's compliance in accordance with this Paragraph 11.2 the Authority may take such steps and perform such analysis as it considers necessary (including the assessment by third party independent auditors) to assess whether best value for money has been or will be achieved in accordance with Clause 5.2 (Standard of Services).	
SERVICE CATALOGUE	12.1	The Service Catalogue shall be developed and agreed and maintained in accordance with Part 13 of Schedule 2.1 (Service Requirements - Information Technology Service Management).	Schedule 4.1 Organisation and Governance Section: 7.16 Retrospective Change Paragraph: 7.16.4
	12.2	The cost of delivering and maintaining the Service Catalogue shall be borne by the Contractor	
	12.3	The Service Catalogue includes an impact assessment for each deliverable change specified in it. Where applicable such impact assessments shall be relied on by the JCAB in assessing requests for Operational Change.	
APPENDIX 1 **Categories of Change**	1	The JCAB shall categories each Change Request as one of the following categories: (a) a "Standard Change", which consists of all Operational Change (but excluding Transformational Change) and, where agreed by the JCAB, Contract Change relating to the scope of the Service Catalogue. Standard Changes are made on an ad hoc basis so are deliverable out of Release; (b) a "Minor Change", which consists of all low risk Contract Change (as assessed and agreed by the JCAB) that requires no more than 20 days to develop and deliver. Minor Changes are made on an ad hoc basis so are delivered out of Release;	Schedule 4.1 Organisation and Governance Section: 7.6 Change Delivery

		(c) a "Normal Change", consists of all medium risk Contract Change (as assessed and agreed by the JCAB). Delivery of a Normal Change shall be via a Minor Release; and (d) a "Major Change", which consists of all high risk and complex Contract Change (as assessed and agreed by the JCAB). Delivery of a Major Change shall be via a Major Release.	
STANDARD CHANGE	2.1	An Impact Assessment for a Standard Change (except where a Change relates to the scope of the Service Catalogue and an Operational Change to the Standards) shall be delivered within timescales to be agreed with the Authority (Change Manager).	
	2.2	An Impact Assessment for a Contract Change which relates to the scope of the Service Catalogue shall be delivered within 10 Working Days of the Change being accepted into the Service Catalogue.	
	2.3	An Impact Assessment for an Operational Change to the Standards shall be delivered within 20 Working Days of the Change being accepted into the Service Catalogue.	
	2.4	A Standard Change shall be implemented within 10 Working Days of approval of the Change Request by the JCAB.	
	2.5	The Contractor shall employ a consistent working practice to ensure all Standard Changes are deployed in accordance with the Service Operations Manual.	
	2.6	Standard Change will not require review by the JCAB, unless otherwise requested by the Authority.	
MINOR CHANGE	3.1	An Impact Assessment for a Minor Change shall be delivered within 10 Working Days of approval at the JCAB.	
	3.2	A Minor Change shall be implemented within 30 Working Days of receipt of an approved Change Authorisation Note	
	3.3	The Change may be delivered as an out of release change or via a Minor Release (in accordance with Paragraph 5.9 (Release Categories) of Appendix 2 of Part 13, Annex M to Schedule 2.1 (Service Requirements - Information Technology Service Management) depending on timelines and testing requirements.	
	3.4	The Contractor shall employ a consistent working practice to ensure all Minor Changes are deployed in accordance with the Service Operations Manual.	
NORMAL CHANGE	4.1	An Impact Assessment for Normal Change shall be delivered within 15 Working Days of approval at the JCAB.	

	4.2	A Normal Change shall be implemented within 3 months of receipt of an approved Change Authorisation Note.	
	4.3	The Contractor shall implement and manage the process that enables Normal Change to be delivered in accordance with the agreed timelines and standards.	
MAJOR CHANGE	5.1	An Impact Assessment for Major Change shall be delivered within the timescales agreed and recorded in the Project Management Plan.	
	5.2	A Major Change shall be implemented in accordance with the delivery methodology and timeline as agreed by the JCAB and on receipt of an approved Change Authorisation Note.	
	5.3	In addition to an Impact Assessment the Contractor shall provide, manage and maintain all documentary deliverables in accordance with the agreed project management framework and delivery methodology for each Change. This shall include, but is not limited to: (a) Project Summary; (b) Project Initiation Document; (c) Project Management Plan; (d) Risk Register; (e) Testing strategy; and (f) Stakeholder Management Plan.	
Schedule 8.6 (BCDR)			
PART 1: BCDR PLANS PURPOSE OF THIS SCHEDULE	1.1	This Schedule sets out the requirements to: (a) ensure the continuity of Critical Business Functions and Outputs in the event of a disaster or disruptive event (including where caused by an Insolvency Event of the Contractor, any Key Sub-Contractor and/or any Contractor Group member) via the implementation of Business Continuity (BC), Disaster Recovery (DR) and/or Insolvency Continuity (IC) procedures; (b) ensure measures are taken to introduce resilience to business systems, processes and operations; and (c) develop, maintain and where appropriate, invoke BCDR Plans	Schedule 4.1 - Common Technical and Enabling Services Section: 13.3 Service Overview
TRANSITION ARRANGEMENTS	2.1	Within 40 days from the Operational Service Commencement Date, the Contractor shall review, validate and, where necessary, update the BCDR Plans for the Services delivered immediately prior to the Effective Date. If updating such plans, the Contractor shall ensure that all such BCDR Plans comply with the requirements set out in this Schedule.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.4 Transition Arrangements (2)

	2.2	The Contractor shall seek to obtain the approval of the Authority in respect of updated plans within the timescale and following receipt of the BCDR Plans from the Contractor, the Authority shall: (a) review and comment on the draft BCDR Plans as soon as reasonably practicable; and (b) notify the Contractor in writing that it approves or rejects the draft BCDR Plans no later than 20 Working Days after the date on which the BCDR Plans are first delivered to the Authority.	
	2.3	If the Authority agrees the draft BCDR Plans, the Contractor shall maintain and adhere to such BCDR Plans (as amended or reformatted from time to time) until such time as they are no longer required, by agreement with the Authority.	
	2.4	If the Authority rejects a draft BCDR Plan: (a) the Authority shall inform the Contractor in writing of its reasons for its rejection; and (b) the Contractor shall then revise the rejected draft BCDR Plan(s) (taking account of the Authority's comments) and shall re-submit revised draft BCDR Plan(s) to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. (c) The provisions of this Paragraph 2.4 shall apply again to any resubmitted draft BCDR Plan. (d) Either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.	
	2.5	The Contractor shall ensure that the appropriate BCDR Plan(s) exist for all Contractor Premises and that each plan details the BC and/or DR arrangements in respect of the Critical Business Functions and Outputs from the relevant Contractor Premises.	
	2.6	During the performance of the Transition Services, the Contractor shall provide all such support, co-operation and information to enable the Authority to update the organisational Business Continuity Management Strategy, which shall be in place no later than 1 month prior to the Operational Service Commencement Date.	
BC, DR AND IC PLANNING - GENERAL PRINCIPLES AND REQUIREMENTS	3.1	To the extent compliance is applicable within the parameters and of this Agreement, the Contractor shall ensure that BC, DR and IC management and the BCDR Plans comply with and adhere to: (a) the organisational Business Continuity Management Strategy (including with any rules or guidance set out therein);	Schedule 4.1 - Common Technical and Enabling Services Section: 13.5 BC, DR and IC Planning – General Principles and Requirements (3)

		(b) JSP 440 (Part 2 Leaflet 16); (c) ISO 22301/22313 to which the BC arrangements within JSP 440 (Part 2 Leaflet 16) are aligned; and (d) ISO 27031 which provide guidelines for ICT readiness for BC,	Section: 13.18 Compliance to the ISO 22301 standard Section: 13.19 Business Continuity Management support software Section: 13.20 Systems architecture and resilience design Section: 13.26 Technical resilience methodology
	3.2	The BCDR Plans shall detail the processes and arrangements which the Contractor shall put in place and follow to ensure the response, continuity and recovery of Critical Business Functions and Outputs following a disaster or disruptive event (including where caused by an Insolvency Event of the Contractor, any Key Sub-Contractor and/or any Contractor Group member). The BCDR Plans shall also: (a) set out method(s) of recovering and/or updating data during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity; (b) identify risks arising from an Insolvency Event of the Contractor, any Key Sub-Contractor and/or Contractor Group member; and (c) detail the provision of any interim services necessary to mitigate the impact of such failure until the services are fully recovered,	
	3.3	The Contractor shall ensure that the BCDR Planning methodology of its Sub-Contractors do not conflict in any adverse way with the organisational Business Continuity Management Strategy detailed in Paragraph 3.1 above.	
	3.4	The Contractor shall ensure that the impact on the Services or to the Authority in the event of a disaster or disruptive event is minimised as far as is reasonably possible.	
	3.5	Business recovery shall be compliant with the RTO established by Business Impact Analysis, as outlined in this Schedule or as set out in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability).	
	3.6	BCDR Plans production should be directed by a BCDR Planning Lifecycle Schedule based on pre-determined 'from' and 'to' calendar dates for each BC and IC activity including: Business Impact Analysis, Risk Assessment, BCDR Plans production, BCDR Plans exercise/test and BCDR Plans release. The Contractor will provide a written, forward looking Schedule (focussing on activity on a rolling 12-month basis).	

	3.7	BC, DR and IC planning shall take into account links and interoperability with any related Authority, Contractor, Sub-Contractor or Third-Party Contractor BC/DR/IC business activity ensuring interdependencies are notified and understood by all relevant parties with collaborative BC, IC and/or DR planning and BC/DR/IC measures put in place across identified links and where interdependencies and interoperability is critical to the output or process.	
	3.8	Having been identified by Risk Assessment or BC, IC and/or DR exercise/test, the vulnerabilities to Critical Business Functions and Outputs should be subject to proactive resilience measures and appropriate Risk Management, whether by technical or other means thus increasing levels of confidence and ultimately system/process availability.	
BUSINESS IMPACT ANALYSIS AND RISK ASSESSMENT	4.1	The Contractor shall, prior to the production of the BCDR Plan, complete a Business Impact Analysis and Risk Assessment on all Contractor Systems and Contractor managed outputs/services, the product of which will determine which outputs/services are deemed to be Critical Business Functions and Outputs and which are less critical and will highlight risk and single points of failure.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.6 Business Impact Analysis and Risk Assessment (4) Section: 13.21 Risk Management
	4.2	Business Impact Analysis and Risk Assessment are to be completed with the following frequencies: (a) at least annually in accordance with review periods for each output/service provision within the extant BCDR Planning Lifecycle Schedule; (b) after Significant organisational change such as changes to the Contractor Group structure and within 30 days of a Corporate Change Event; (c) within 14 days of a Financial Distress Event; (d) after Significant business process or system change; and (e) after Significant disruption to output/services requiring activation of BC measures.	
BCDR PLANS	5.1	The Contractor shall produce, maintain and review BCDR Plans for all Contractor managed Critical Business Functions and Outputs and for Contractor Premises or Authority Premises (where the Contractor staff make up the majority of staff).	Schedule 4.1 - Common Technical and Enabling Services Section: 13.7 BCDR Plans (5) Section: 13.16 Business Continuity Planning Approach and Methods
	5.2	The Authority shall produce, maintain and review BCDR Plans where: (a) the system/process is not managed by the Contractor; or	

		(b) for non-technical ad hoc BCDR Plans aided by the Contractor, where a joint solution is required (e.g. for the Pandemic Contingency Plan).	
	5.3	Where site/location focussed plans are produced, the Contractor will ensure the main Contractor location is subject to BC and IC planning and the Contractor shall provide input as requested by the Authority into other sites/locations BC Plans and IC Plans where the Contractor has operational staff.	
	5.4	Where not already covered by appropriate contingency planning, the Contractor shall produce ad hoc BC, IC and/or DR Plans on a requirements basis e.g. in anticipation of Significant disruption caused by unforeseen industrial action and unforeseen environmental issues. The Contractor shall provide input into the Pandemic Contingency Plan on request and as required by the Authority.	
	5.5	The Contractor shall produce and maintain a Register of all Contractor produced/managed BCDR Plans for reference and monitoring purposes. This BCDR Plans Register shall be updated on an ongoing basis and/or at least monthly and be made available to the Authority on request and/or on the last day of the calendar month.	
BCDR PLANS - INVOCATION AND RESPONSE	6.1	In the event of a loss of any critical part of the Services, a disaster or disruptive event (or of the Contractor's reasonable expectation of such a loss), the Contractor shall immediately initiate a response in accordance with the BC and DC provisions of the relevant BCDR Plan, deploying sufficient resources from invocation to incident closure to ensure business system/process recovery. The Contractor shall ensure that normal Service provision is resumed in accordance with timescales established by Business Impact Analysis, the requirements of the relevant BCDR Plans and/or as set out in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability). The Contractor shall inform the Authority promptly of this action.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.8 BCDR Plans – Invocation and Response (6) Section: 13.23 Approach to crisis/major incident management and communications
	6.2	The Contractor shall maintain the flow of crisis/incident information to the Authority from invocation to crisis/incident closure and the Contractor shall respond to all requests for crisis/incident information from the Authority. The Authority reserves the right to convene crisis management meetings with a representative of the Contractor required to attend (unless agreed otherwise between the Parties). The Authority will be responsible for invoking any BCDR Plans for systems/process solely managed by the Authority.	

	6.3	On crisis/incident closure, the Contractor shall provide a report within 15 Working Days outlining crisis/incident details including location, the system/process affected, business impacts, response and recovery timeline, lessons learned and an action plan outlining any required remediation measures.	
	6.4	The Insolvency Continuity Plan element of the BCDR Plans, including any linked elements in other parts of the BCDR Plans, shall be invoked by the Contractor: (a) where an Insolvency Event of a Key Sub-Contractor and/or Contractor Group member (other than the Contractor) could reasonably be expected to adversely affect delivery of the Services; and/or (b) where there is an Insolvency Event of the Contractor and the insolvency arrangements enable the Contractor to invoke the plan.	
BCDR PLANS – BCDR TEST	7.1	The Contractor shall perform a BCDR Test on all the BCDR Plans with the following frequencies: (a) at least annually in accordance with the BCDR Plan review periods for each output/service provision within the extant BCDR Planning Lifecycle Schedule; (b) after Significant organisational change such as changes to the Contractor Group structure and within 30 days of a Corporate Change Event; (c) within 14 days of a Financial Distress Event; (d) after Significant Operational Change; (e) after Significant disruption to Services requiring activation of BC measures; (f) in anticipation of a likely future disaster or disruptive event which has increased the likelihood of plan invocation; and (g) the earlier of either 3 months prior to the expiry of this Agreement or within 1 month of the issue of a Termination Notice by either Party in accordance with the Agreement.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.9 BCDR Plans – BCDR Test (7) Section: 13.22 Approach to business continuity testing and incorporating lessons learnt Section: 13.27 Annual Disaster Recovery Testing
	7.2	The Contractor shall produce and maintain a Schedule of planned BCDR Tests, containing a 12-month rolling forecast of the times and dates on which each of the BCDR Plans shall carried out, and make it available to the Authority on request and, in any event, on the last day of each calendar month.	
	7.3	The Contractor shall undertake and manage BCDR Tests. Where a BCDR Test is considered by the Contractor to be Significant or at the	

		request of the Authority, the Contractor will undertake the exercise/test in full consultation with the Authority and comply with the reasonable requirements of the Authority in conducting the test. For such BCDR Tests Contractor shall provide the Authority with adequate advance notification of the BCDR Test, provide written confirmation of the exercise/test scope, aims, objectives, methodology and a risk assessment carried out against the practical requirements of the exercise/test. For each Significant BCDR Test the Contractor shall invite a representative of the Authority or its nominee to witness the test, especially where it is a test relating to ICT.	
	7.4	If the Authority requires an additional BCDR Test of a BCDR Plan, it shall give the Contractor written notice and the Contractor shall conduct the test in accordance with the Authority's requirements and the relevant provisions of the BCDR Plan. The Contractor's costs of the additional test shall be borne by the Authority unless the BCDR Plan fails the additional BCDR Test, in which case the Contractor's costs of that failed test shall be borne by the Contractor.	
	7.5	The Contractor shall ensure that any use by any Sub-contractor of Authority Data in BCDR Testing is first approved with the Authority. Copies of Authority Data used in any such BCDR Test shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.	
	7.6	The Contractor shall ensure that each BCDR Test minimises any downtime or other adverse impact to the Operating environment.	
	7.7	The Contractor shall, within 15 Working Days of the conclusion of each BCDR Test, provide to the Authority a report setting out: (a) the outcome of such BCDR Test; (b) any failures in any BCDR Plan (including such BCDR Plan's procedures) revealed by the BCDR Test; and (c) the Contractor's proposals for remedying any such failures.	
	7.8	Following each BCDR Test, the Contractor shall take all measures requested by the Authority, (including requests for the re-testing of the BCDR Plan) to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Contractor, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.	
	7.9	For the avoidance of doubt, the carrying out of a BCDR Test of any BCDR Plan (including a test of such BCDR Plan's procedures) shall not	

		relieve the Contractor of any of its obligations under this Agreement save to the extent provided for elsewhere in this Agreement or in the BCDR Plan.	
BCDR PLANS - REVIEW AND MAINTENANCE	8.1	The Contractor shall conduct BCDR Reviews with the following frequencies: (a) as a minimum, at least annually or more frequently should the output criticality or sensitivity to time delay and/or external factors determine so in the Contractors reasonable opinion (acting in accordance with good industry practice); (b) within 1 month of any BCDR Plan (or any part) having been invoked; (c) as soon as is practicable and in any event within 1 month of the following: (i) a Significant system/process/organisation change including a change to the Contractor Group structure; (ii) an Insolvency Event of the Contractor, any Key Sub-Contractor and/or any Contractor Group member; (iii) an improvement and/or update to the BCDR Plans; (iv) following a BCDR Test; (v) a relocation of the IT Environment; and/or (vi) the Parties entering into a Change Authorisation Note; and/or (d) in anticipation by either Party of a likely future disaster or disruptive event which may increase the likelihood of plan invocation.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.1 BCDR Plans – Review and Maintenance (8) Section: 13.17 Business Continuity and Disaster Recovery plan(s) planning and maintenance processes
	8.2	Where the Authority requests any additional BCDR Reviews (over and above those provided for in Paragraph 8.1) it shall notify the Contractor in writing and the Contractor shall conduct such BCDR Reviews in accordance with the Authorities written requirements. The reasonable costs of both Parties for any such additional BCDR Reviews will be met by the Authority unless such BCDR Review has been requested by the Authority to rectify a deficiency identified in the BCDR Plans in which case, the Contractor shall bear its own costs and reimburse the Authority for the any Authority costs reasonably incurred which arise out of such a review.	
	8.3	The Authority shall retain the right to be an integral part of the BCDR Review process requesting reasonable amendments, deletions or additions as required. The Authority shall also retain the right to formally endorse the BCDR Plan prior to its release (i.e. provide sign-off indicating plan release or re-release may take place).	

	8.4	Each BCDR Review pursuant to Paragraph 8.1 shall be a review of the procedures and methodologies set out in the BCDR Plans and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan. The BCDR Reviews 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 Plans. The review and subsequent release shall be completed by the Contractor within the period required by the BCDR Plans (no later than 1 month after the target release date, the target release date being 12 months after the previous release date except when subject to an agreed deferral) or if no such period is required, within such period as the Authority shall reasonably require.	
	8.5	The Contractor shall, within 20 Working Days of the conclusion of each BCDR Review, if requested by the Authority, provide to the Authority a report of the BCDR Review ("the BCDR Review Report") setting out: (a) the findings of the BCDR Review; (b) any changes to the risk profile associated with the Services; and (c) the Contractor's proposals for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan following the review detailing the impact (if any and to the extent that the Contractor can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any Services or systems.	
	8.6	Any changes which may be required to the BCDR Plan arising from the review of the BCDR Review Report shall be agreed between the Parties in accordance with the Change Control Procedure. Such changes shall be Contractor funded unless it can be demonstrated by the Contractor to the reasonable satisfaction of the Authority that the changes are required solely because of material change to the Services and/or the Authority requirements.	
BC, IC AND DR – ACTIVITY REPORTS AND MANAGEMENT INFORMATION	9.1	A BCDR Report shall be provided to the Authority on the last Working Day of the calendar month and will include information on the following categories of Contractor BC, IC and DR activity: (a) site or location BC and IC planning; (b) ICT DR and business process BC and IC planning; (c) any BCDR Tests carried out; (d) BC and IC culture and awareness;	Schedule 4.1 - Common Technical and Enabling Services Section: 13.11 BC, IC and DR – Activity Reports and Management Information (9)

		(e) the risks to BC and IC; (f) the occurrence of any BC, IC and DR incidents; and (g) general update/commentary on BC, IC and DR.	
	9.2	The Contractor shall respond to ad hoc requests for Management Information from the Authority within Authority declared timeframes. Information can relate to all aspects of BC, IC or DR activity and may be provided in response to requests by internal or external sources. Responses can be in the form of a Microsoft Powerpoint presentation, formal reports and formal/informal briefings.	
	9.3	Contractor Subject Matter Expert(s) shall attend the following scheduled BC and IC meetings: (a) **Business Continuity Steering Group**. This meeting should be attended by the Contractor BC and IC Subject Matter Expert and a summary report of Significant historical and forward-looking Contractor BC, IC and DR activity shall be provided by the Contractor to attendees at least 1 week prior to the meeting. (b) **Location BC Working Groups (where applicable)**. This meeting should be attended by the Contractor BC and IC Subject Matter Expert and representatives from key Contractor business teams and, where the Contractor staff make up the majority of operational staff present on the site the meeting is being held, the Contractor shall provide the Chairperson and Secretary.	
BUSINESS CONTINUITY TRAINING	10.1	The Contractor shall ensure that all permanent staff and staff contracted for 6 months or more complete Authority's 'Business Continuity Induction Training' within 1 month of employment start date or within 6 months of the Effective Date and every 5 years thereafter.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.12 Business Continuity Training (10)
INSOLVENCY CONTINUITY PLAN	11.1	The Insolvency Continuity Plan shall be designed by the Contractor to permit continuity of the business operations of the Authority supported by the Services through continued provision of the Services following an Insolvency Event of the Contractor, any Key Sub-Contractor and/or any Contractor Group member with, as far as reasonably possible, minimal adverse impact.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.13 Insolvency Continuity Plan (11)
	11.2	The Insolvency Continuity Plan shall include the following: (c) communication strategies which are designed to minimise the potential disruption to the provision of the Services, including key contact details in respect of the supply chain and key contact details for operational and contract Contractor Personnel, Key Sub-Contractor personnel and Contractor Group member personnel;	

		(d) identification, explanation, assessment and an impact analysis of risks in respect of dependencies between the Contractor, Key Sub-contractors and Contractor Group members where failure of those dependencies could reasonably have an adverse impact on the Services; (e) plans to manage and mitigate identified risks; (f) details of the roles and responsibilities of the Contractor, Key Sub-contractors and/or Contractor Group members to minimise and mitigate the effects of an Insolvency Event of such persons on the Services; (g) details of the recovery team to be put in place by the Contractor (which may include representatives of the Contractor, Key Sub-contractors and Contractor Group members); and (h) sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of an Insolvency Event of the Contractor.	
PART 2: CORPORATE RESOLUTION PLANNING SERVICE STATUS AND CONTRACTOR STATUS	1.1	This Agreement is a Critical Service Contract.	Schedule 4.1 - Common Technical and Enabling Services Section: 13.14 Part 2: Corporate Resolution Planning
	1.2	The Contractor shall notify the Authority in writing within 5 Working Days of the Effective Date and throughout the Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier.	
PROVISION OF CORPORATE RESOLUTION PLANNING INFORMATION	2.1	Paragraphs 2 to 4 of this Part 2 shall apply if this Agreement has been specified as a Critical Service Contract under Paragraph 1.1 of this Part 2 or the Contractor is or becomes a Public Sector Dependent Supplier.	
	2.2	Subject to Paragraphs 2.6, 2.10 and 2.11 of this Part 2: (a) where this Agreement is a Critical Service Contract, the Contractor shall provide the Relevant Authority with the CRP Information within 60 days of the Effective Date; and (b) except where it has already been provided in accordance with Paragraph 2.2(a) of this Part 2, where the Contractor is a Public Sector Dependent Supplier, it shall provide the Relevant Authority with the CRP Information within 60 days of the date of the Relevant Authority's request.	
	2.3	2.3 The Contractor shall ensure that the CRP Information: (a) is full, comprehensive, accurate and up to date; (b) is split into two parts: (i) Group Structure Information and Resolution Commentary;	

		(ii) UK Public Service / CNI Contract Information, and is structured and presented in accordance with the requirements and explanatory notes set out at Annex I of the latest published version of the Resolution Planning Guidance published by the Cabinet Office Government Commercial Function and available at https://www.gov.uk/government/publications/the-outsourcing-playbook and contains the level of detail required (adapted as necessary to the Contractor's circumstances); (c) incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Relevant Authority to understand and consider the information for approval; (d) provides a clear description and explanation of the Contractor Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and (e) complies with the requirements set out at Appendix I (Group Structure Information and Resolution Commentary) and Appendix 2(UK Public Sector / CNI Contract Information) respectively.	
	2.4	Following receipt by the Relevant Authority of the CRP Information pursuant to Paragraphs 2.2, 2.8 and 2.9 of this Part 2, the Contractor and the Relevant Authority shall discuss in good faith the contents of the CRP Information and: (a) where the Authority is the Relevant Authority, the Authority shall; and (b) where the Cabinet Office Markets and Suppliers Team is the Relevant Authority, the Authority shall use reasonable endeavours to procure that the Cabinet Office Markets and Suppliers Team shall, no later than 60 days after the date on which the CRP Information was delivered by the Contractor either provide an Assurance to the Contractor that it approves the CRP Information or that it rejects it.	
	2.5	If the Relevant Authority rejects the CRP Information: (a) the Authority shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Contractor in writing of its reasons for its rejection; and (b) the Contractor shall revise the CRP Information, taking reasonable account of the Relevant Authority's comments, and shall re-submit the CRP Information to the Relevant Authority for approval within 30 days of the date of the Relevant Authority's rejection. The provisions of Paragraph 2.3 to 2.5 of this Part 2 shall apply again to any resubmitted	

		CRP Information provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.	
	2.6	Where the Contractor has already provided CRP Information to a Department (or, in the case of a Strategic Supplier, to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that Department (or, in the case of a Strategic Supplier, from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid, the Contractor shall not be required to provide the CRP Information or updated CRP Information under Paragraphs 2.2 and 2.8(a) to 2.8(c) of this Part 2 if it provides a copy of the Valid Assurance to the Authority on or before the date on which the CRP Information would otherwise have been required.	
	2.7	An Assurance shall be deemed Valid for the purposes of Paragraph 2.6 of this Part 2 if: (a) in respect of the Contractor's obligations under Paragraph 2.2: (i) the CRP Information on which the Assurance was based was provided to the Department providing the Assurance (or, in the case of Strategic Suppliers, to the Cabinet Office Markets and Suppliers Team) within the 12 months prior to the deadline by which the CRP Information would otherwise have been required under Paragraph 2.2; and (ii) no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if this Agreement had then been in force) have occurred since the date on which the CRP Information was provided; and (b) in respect of the Contractor's obligations under Paragraphs 3.8(a) to 3.8(c) the CRP Information on which the Assurance was based was provided to the Department providing the Assurance (or, in the case of Strategic Suppliers, to the Cabinet Office Markets and Suppliers Team) after the date of the event triggering the obligation to provide the CRP Information under Paragraphs 2.8(a) to 3.8(c).	
	2.8	Subject to Paragraph3.6, if this Agreement is a Critical Service Contract, the Contractor shall provide an updated version of the CRP Information (or, in the case of Paragraph 2.8(c) of this Part 2 its initial CRP Information) to the Relevant Authority: (a) within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 2.11 of this Part 2) unless the Contractor is relieved of the consequences of the Financial Distress	

		Event under Paragraph 7.1 (Primacy of Credit Ratings) of Schedule 7.4 (Financial Distress); (b) within 30 days of a Corporate Change Event unless not required pursuant to Paragraph 2.10; (c) within 30 days of the date that: (i) the credit rating(s) of each of the Contractor and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 2.10; or (ii) none of the credit rating agencies specified at Paragraph 2.10 hold a public credit rating for the Contractor or any of its Parent Undertakings; and (d) in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Relevant Authority (whichever is the earlier), unless: (i) updated CRP Information has been provided under any of Paragraphs 2.8(a), 2.8(b) or 2.8(c) since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 2.8(d); or (ii) unless not required pursuant to Paragraph 2.10.	
	2.9	Where the Contractor is a Public Sector Dependent Supplier and this Agreement is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 2.8(a) to (d) of this Part 2, the Contractor shall provide at the request of the Relevant Authority and within the applicable timescales for each event as set out in Paragraph 2.8 (or such longer timescales as may be notified to the Contractor by the Authority), the CRP Information to the Relevant Authority.	
	2.10	Where the Contractor or a Parent Undertaking of the Contractor has a credit rating of either: (a) Aa3 or better from Moody's; (b) AA- or better from Standard and Poors; (c) AA- or better from Fitch; the Contractor will not be required to provide the CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Contractor is relieved of the consequences of the Financial Distress Event under Paragraph 7.1 (Primacy of Credit Ratings) of Schedule 7.4 (Financial Distress)) or (ii) the Contractor and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the Contractor	

		shall provide the updated version of the CRP Information in accordance with Paragraph 2.8.	
	2.11	Subject to Paragraph 4, where the Contractor demonstrates to the reasonable satisfaction of the Relevant Authority that a particular item of CRP Information is highly confidential, the Contractor may, having orally disclosed and discussed that information with the Relevant Authority, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Contractor shall promptly provide the relevant information to the Relevant Authority to the extent required under Paragraph 2.8.	
TERMINATION RIGHTS	3.1	The Authority shall be entitled to terminate this Agreement under Clause 38.1(b) (Termination by the Authority) if the Contractor is required to provide CRP Information under Paragraph 2 of this Part 2 and either: (a) the Contractor fails to provide the CRP Information within 4 months of the Effective Date if this is a Critical Service Contract or otherwise within 4 months of the Relevant Authority's request; or (b) the Contractor fails to obtain an Assurance from the Relevant Authority within 4 months of the date that it was first required to provide the CRP Information under this Agreement.	
CONFIDENTIALITY AND USAGE OF CRP INFORMATION	4.1	The Authority agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Contractor and/or Contractor Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.	
	4.2	Where the Relevant Authority is the Cabinet Office Markets and Suppliers Team, at the Contractor's request, the Authority shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Contractor containing terms no less stringent than those placed on the Authority under Paragraph 4.1 of this Part 2 and Clause 26 (Confidentiality).	
	4.3	The Contractor shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Relevant Authority pursuant to Paragraph 2 of this Part 2 subject, where necessary, to the Relevant Authority entering into an appropriate confidentiality agreement in the form required by the third party.	

	4.4	Where the Contractor is unable to procure consent pursuant to Paragraph 4.3 of this Part 2, the Contractor shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by: (a) redacting only those parts of the information which are subject to such obligations of confidentiality; and/or (b) providing the information in a form that does not breach its obligations of confidentiality including (where possible) by: (i) summarising the information; (ii) grouping the information; (iii) anonymising the information; and (iv) presenting the information in general terms.	
	4.5	The Contractor shall provide the Relevant Authority with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Contractor is legally permitted to do so.	
APPENDIX I **Group Structure Information and Resolution Commentary**	1	The Contractor shall:	
	1.1	provide sufficient information to allow the Relevant Authority to understand the implications on the Contractor Group's UK Public Sector Business and CNI contracts listed pursuant to Appendix II if the Contractor or another member of the Contractor Group is subject to an Insolvency Event;	
	1.2	ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Contractor Group; and	
	1.3	provide full details of the importance of each member of the Contractor Group to the Contractor Group's UK Public Sector Business and CNI contracts listed pursuant to Appendix II and the dependencies between each.	
APPENDIX II **UK Public Sector / CNI contract Information**	1	The Contractor shall:	
	1.1	provide details of all agreements held by members of the Contractor Group where those agreements are for goods, services or works provision and: (a) are with any UK public sector bodies including: central Government departments and their arms-length bodies and agencies,	

		non-departmental public bodies, NHS bodies, local authorities, health bodies, police fire and rescue, education bodies and the devolved administrations; (b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Appendix II and where the member of the Contractor Group is acting as a key subcontractor under the agreement with the end recipient; or (c) involve or could reasonably be considered to involve CNI;	
	1.2	provide the Relevant Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key subcontracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link.	