FUTURE SERVICE DELIVERY CONTRACT

SCHEDULE 2.1

PART 13 - IT SERVICE MANAGEMENT

CONTENTS

Clause	Heading	Page
1	DEFINITIONS	3
2	INTRODUCTION	6
3	ADOPTING THE ITIL FRAMEWORK	7
4	THE SERVICE OPERATION MANUAL (SOM)	7
5	TRANSFORMATION TO PSEUDO SIAM, AND SIAM	9

1 DEFINITIONS

1.1 In this Part 13 of Schedule 2.1, the following definitions shall apply:

Architecture Management Office (AMO)	shall have the meaning as set out in ITIL;
Authority Design Assurance	the Authority function which provides Authority domain knowledge and expertise to the Joint Architecture Governance framework;
Capacity	capacity of Services and the supporting IT Environment, systems and services is able to deliver the agreed Performance Indicators in an efficient and timely manner;
Capacity Plan	a plan that outlines the resources needed to support the required business outcomes, as further detailed in ITIL;
Capacity Report	shall have the meaning as set out in ITIL;
Change Delivery Strategy	a document detailing a defined set of project delivery methods to be adopted to ensure the effective delivery of Change (including but not limited to RACI matrices, process definitions, and process maps);
Change Management System	a workflow based automated system for the management of all Change Requests;
CMMI	Capability Maturity Model Integration;
Configuration Items	shall have the meaning as set out in ITIL;
Configuration Management Database	shall have the meaning as set out in Schedule 8.2 (Change Control Procedure);
Critical Design Review	a technical review of Change that occurs after the completion of Service Design and prior to Testing in order to demonstrate that the maturity of the product design is appropriate to support full scale integration and Testing and that the deliverable(s) meet the requirements as detailed within the relevant Change Request(s) and are within the agreed time and cost constraints;
Enterprise Architecture	the practise of undertaking enterprise-wide ICT analysis, design, planning and implementation, aligned to the Authority's business objectives;
Event Management	the management processes and measures in place to indicate when something is not functioning correctly,

	leading to an Incident being logged which must identify Events, analyse and determine the appropriate control activity or action to prevent an Incident and/or service interruption;
Existing Estate Architecture	the extant IT Environment technical estate;
Forward Schedule of Change	a document detailing all Changes which are agreed to be implemented which is used by the Parties to plan, coordinate and monitor the delivery of such Changes into live operations as agreed with and in collaboration with the Authority. For the avoidance of doubt this includes all Release and Out of Release deliverables;
IT Services	those Services delivered using ICT;
ITSCM	IT Service Continuity Management;
ITSM	the processes and procedures performed by the Contractor to design, plan, operate and control the ICT Services;
ITSM Maturity Assessments	an independent assessment of the Maturity of the ITSM through CMMI (or another recognised industry standard provider) intended to ensure continual improvement of the ITSM capability and provide the Authority with a measure of the progress of operational Maturity of both the Contractor's and Authority's ITSM capability, to be assigned an Maturity Level measured against each Maturity Characteristics;
ITSM Plan	a plan of the development and implementation of all ITSM processes, taking input from the ITSM Maturity Assessment;
Joint Architecture Board	a control and approval board within the JAG framework, consisting of Architecture Management Office and Authority Design Assurance representatives, which enforces and oversees the Enterprise Architecture Management;
Joint Architecture Governance	the framework under which the Authority Design Assurance and Architecture Management Office work, to collaboratively define and enforce the governance of the Enterprise Architecture;
Maturity	the maturity of the ITSM capability as independently assessed against the Maturity Levels;
Maturity Characteristics	the characteristics of Maturity of the ITSM capability, as set out in Paragraph 2 of Appendix 1 (Service Maturity

	Assessment and Development);
Maturity Levels	the levels of Maturity of the ITSM capability as set out in Paragraph 1 of Appendix 1 (Service Maturity Assessment and Development);
Problem	the underlying root cause of the Incident, which shall have the meaning as set out in ITIL;
Pseudo SIAM	the scope of the SIAM capability that the Contractor is expected to establish during the Term;
RACI	Responsible, Accountable, Consulted and Informed;
Resolver Group	shall have the meaning as set out in ITIL;
Risk Management	a process which supports the decision-making process to accurately assess risks and the associated impacts and potential benefits of actions in relation to the ability to support and deliver the Services. Such Rick Management enables the identification of positive and negative risks to be analysed and a course of action to be determined based on value and impact to the Service Lifecycle, ensuring that the best possible outcome can be achieved;
Operational Readiness Review	a rigorous, systematic and documented examination of a new Service or Change(s) to a Service prior to the Service's acceptance into Operations to assure stakeholders that all functional and/or non-functional requirements have been met, and in order to identify consequential risks of introducing the changed Service;
Service Assets	shall have the meaning as set out in ITIL;
Service Catalogue	a catalogue that provides summarised definitions of all Services and their components to support Service Portfolio Management and which further allows for Operational Change and Contract Change Service components and items to be provisioned, as defined in Service Catalogue Management in Part 13 of Schedule 2.1;
Service Catalogue Management	shall have the meaning as set out in ITIL;
Service Event	an outcome or occurrence on a system or process as part of the performance of the Services, which may be benign (for example, an audit log message of a successful job completion) or may be the manifestation of an Problem that

	will become an Incident;
Service Improvement Plan	the documented activities to be undertaken and their delivery timeline, to resolve a service delivery issue or implement an improvement opportunity under the ITIL process of 'Continual Service Improvement';
Service Lifecycle	shall have the meaning as set out in ITIL;
Service Operations Manual	the service operations manual which describes the policies, processes and procedures required by this Schedule and their associated service metrics that define the ITSM processes and functions which are required to manage the Service and will be used to define and measure compliance to the Performance Indicators;
Service Outage	any unplanned period of time during which any of the Services are not available;
Service Portfolio	shall have the meaning as set out in ITIL;
Service Request	shall have the meaning as set out in ITIL;
Service Strategy Plan	a Service Lifecycle based strategy which focuses on maturing and improving the Enterprise Architecture in meeting the transformational and business objectives of the Authority;
SIAM	means Service Integration and Management is an approach to managing multiple suppliers of services and integrating them to provide a single business-facing IT organisation.
Solution Architecture	the practice of defining and describing the architecture of a system to be delivered in context of a specific solution, in compliance with the Joint Architecture Governance framework;
Tower Services	a single defined component of the SIAM Service that can be contracted individually as a viable service in its own right which is co-ordinated and integration with other Tower services will be via the SIAM capability;

2 INTRODUCTION

1.1 This Schedule details the IT Service Management (ITSM) that shall be provided by the Contractor to the Authority. The structure of this Schedule is as follows:

(a) Section 2 summarises the maturity expectations for ITSM, defines the overall requirements for the ITSM Services and provides the common requirements that are expected of all ITSM process areas and functions;

(b) Section 3 describes the Transformation requirements and the SIAM and Pseudo SIAM expectations;

(c) Appendix 1 (Maturity Levels and Maturity Characteristics) sets out the Maturity Levels and associated Maturity Characteristics; and

(d) Appendix 2 (ITSM Requirements) set out the minimum required ITSM requirements for each individual ITSM process and function area.

3 ADOPTING THE ITIL FRAMEWORK

Adopting ITIL to support ICT Services

3.1 The Contractor shall:

(a) implement all ITSM processes and functions as contained in Appendix 2 (ITSM Requirements) and, once approved, in accordance with the Service Operation Manual across all elements of the Services (including the targets, metrics and measures used to provide the Performance Indicators) as its control and delivery mechanism for implementing, managing, delivering and improving the ICT Services;

(b) ensure a measurable progression of Maturity in its ITSM capability in accordance with Annex M (Technical & Applications); and

(c) conduct ITSM Maturity Assessments to assess the Maturity of its ITSM capability.

ITSM Maturity Assessment

3.2 The Contractor shall conduct an ITSM Maturity Assessment on the Operational Service Commencement Date and on each anniversary of the Contract Year thereafter, which shall:

(a) detail the progress in achieving a ITSM Maturity since the last ITSM Maturity Assessment;

(b) provide an assessment on the Contractor and Authority capabilities required to manage the Services to the required Maturity; and

(c) provide recommendations for improvement actions to achieve a progression in ITSM Maturity.

4 THE SERVICE OPERATION MANUAL (SOM)

Approval of the Service Operation Manual

4.1 The Contractor shall submit to the Authority a draft Service Operation Manual within 40 Working Days of the Effective Date.

4.2 The Contractor shall ensure that the draft Service Operation Manual includes (as a minimum):

(a) the requirements set out in Appendix 2 (ITSM Requirements);

(b) an organisational operating model which provides for required Contractor and Authority roles, with defined RACI characteristics;

(c) details of the staff nominated by the Contractor to have responsibility for each process or function within the Service Operation Manual who will act as contact points for the Authority representatives and be 'Subject Matter Experts' in the process or function;

(d) service metrics and Performance Indicators based upon the Contractor's standard offering and the Authority Requirements. Where Performance Indicators are related to ITSM requirements contained in the Service Operations Manual or specifically identified as such by the Authority, such Performance Indicators must be taken as a minimum requirement for the SOM, unless otherwise agreed with the Authority;

(e) the Contractor's approach to the maturing and use of the Service Operation Manual;

(f) a plan for developing the Maturity of the ITSM processes over the course of the Term; and

(g) provide evidence of adherence to all required Maturity characteristics.

4.3 Prior to the submission of the draft Service Operation Manual to the Authority in accordance with paragraph 3.1, the Authority shall have the right:

(a) to review any documentation produced by the Contractor in relation to the development of the Service Operation Manual, including:

(i) details of the Contractor's intended approach to the Service Operation Manual and its development;

(ii) copies of any drafts of the Service Operation Manual produced by the Contractor; and

(iii) any other work in progress in relation to the Service Operation Manual; and

(b) to require the Contractor to include any reasonable changes or provisions in the Detailed Transition Plan.

4.4 Following receipt of the draft Service Operation Manual from the Contractor, the Authority shall:

(a) review and comment on the draft Service Operation Manual as soon as reasonably practicable; and

(b) notify the Contractor in writing that it approves or rejects the draft Service Operation Manual no later than 20 Working Days after the date on which the draft Service Operation Manual is first delivered to the Authority.

4.5 If the Authority rejects the draft Service Operation Manual:

(a) the Authority shall inform the Contractor in writing of its reasons for its rejection; and

(b) the Contractor shall then revise the draft Service Operation Manual (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Service Operation Manual to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Service Operation Manual, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

4.6 If the Authority approves the draft Service Operation Manual, it shall replace the Outline Transition Plan from the date of the Authority’s notice of approval.

Updates to and maintenance of the Service Operation Manual

4.7 Following the approval of the Service Operation Manual by the Authority:

(a) the Contractor shall submit a revised Service Operation Manual to the Authority within 40 Working Days of an ITSM Maturity Assessment; and

(b) without prejudice to Paragraph 3.7(a), the Authority shall be entitled to request a revised Service Operation Manual at any time by giving written notice to the Contractor and the Contractor shall submit a draft revised Service Operation Manual to the Authority within 40 Working Days of receiving such a request from the Authority (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure).

4.8 Any proposed amendments to the Detailed Transition Plan shall not come into force until they have been approved in writing by the Authority.

4.9 Following the submission of any revised Service Operation Manual to the Authority, the Contractor shall, if requested by the Authority, promptly provide training to nominated members of the Authority.

5 TRANSFORMATION TO PSEUDO SIAM, AND SIAM

Provide flexibility in approach and solution

5.1 The Contractor shall provide the Authority with a flexible approach and solution to Transformation of the Services by:

(a) ensuring that the future Tower Service contractors will benefit from SIAM services in the future, supporting systems and solutions should be designed for scalability, as appropriate and for process and technology integration;

(b) ensuring that future Tower Service contractors will be able deliver their components of the SIAM service separated from the other Tower Service contractors, allowing for individual Tower Services to be included and replaced with minimal disruption to the continuity the SIAM services; and

(c) there must be a well-defined strategy for each of the Tower Services to transfer to future Tower Service contractors.

Achieve seamless transition to SIAM via Pseudo SIAM

5.2 The Contractor shall:

(a) maintain business as usual during the Transformation process by ensuring adequate measures and controls are established to ensure seamless operation of all Services before, during and after Transformation;

(b) ensure a transition to a SIAM operating model by developing all Services to facilitate a transition to a multi-supplier environment at the end of the Term by establishing appropriate SIAM capability during the Term;

(c) undertake and complete the development of the SIAM operating model in accordance with the following:

(i) in respect of the Tower Services:

(A) new Tower Services will be instantiated following Transformation of each key service area and such Tower Service construct will span all architecture domains; and

(B) these Tower Services will need to co-exist with existing service constructs until all Transformation activities are complete;

(ii) in respect of the SIAM capability:

(A) the Pseudo SIAM capability will need to be developed from the Service Commencement Date and matured to a state where it can effectively manage integration between current services and the transformed and disaggregated Tower Services as they are delivered;

(B) development should be continuous and when the final tower service is created the Pseudo SIAM capability must be mature and effectively managing service integration across all services;

(C) the transition to a multi-supplier operating model following the expiry of the Term will need to be enabled and supported by the Contractor;

(D) the Contractor must show consideration for this final end state throughout the Term in all Changes that are made to the Service;

(E) transition to a multi-supplier environment must be completed with minimal impact and cost to the Authority; and

(F) the Authority only expect limited process, organisation and governance changes to be required in the transition to a multi-supplier state following the expiry of the Term; and

(G) the Authority requires that all data, application and technology changes would have been made within this Agreement.

(iii) in respect of the Contracting Model following the expiry or termination of the Agreement:

(A) multiple contracts will be let which will be aligned to the Tower Services;

(B) the SIAM capability may be one of those contracted services or alternatively the Authority may assume control of this function. Flexibility is needed within the Contractor's solution to ensure either option is viable; and

(C) a single Supplier of two or more services is not expected to be precluded.

Construct viable disaggregated Tower Services

5.3 The Contractor shall:

(a) ensure each of the disaggregated Tower Services must be viable services in their own right and be able to be operated by a new third party supplier without dependence upon existing Contractor (or third party suppliers of the other disaggregated services), excepting agreed data interfaces which should be fully interoperable with one another as required by the services various integration requirements;

(b) ensure the Tower Services are delivered using standardised, consistent and integrated technology methodology and tooling so that each Tower Service can easily accommodate the transition to a multi-supplier tower service operating model;

(c) ensure that each Tower Service utilises common and cross-functional technology capability (for example, utilising the same data interfacing and integration platform) to allow for inter-dependencies of each Tower Service for future Tower Service suppliers; and

(d) facilitate the future Tower Service suppliers in delivering its component of the Services in a modular way allowing for Tower Services to be included and replaced with minimal disruption to the continuity of end-to-end services to the Authority.

Risk Management Plan

5.4 The Contractor shall manage all risks associated with Transformation by providing a comprehensive risk management plan, which shall include but not limited to:

(a) the Contractor's ability to measure performance of the totality of the Services;

(b) the Contractor's ability to define the scope and specification of each Tower Service;

(c) managing relationships and collaboration between Tower Services;

(d) standardising and modularising services;

(e) lack of ownership as the number of service boundaries are increased;

(f) added complexity of technology or management outweighing benefits;

(g) the risk to Data integrity; and

(h) the risk of 'dilution of knowledge', as barriers go up around each Tower Service; and

(i) ensure such risk management process plans are followed at all times.

APPENDIX 1

Maturity Levels and Process and Maturity Characteristics

1. Maturity Levels: The Maturity Levels for the ITSM capability are as follows:

Maturity Level	Maturity Description
Level 0 Non-existent	• There is no ITSM process in place. • Complete lack of any recognisable ITSM process or the Contractor has not recognised that there is an issue to be addressed.
Level 1 Initial (reactive)	• ITSM process is ad hoc and disorganised. • The Contractor has recognised that issues exist and need to be addressed. • However, there are no standardised ITSM processes operating; there are ad hoc approaches that tend to be applied on an individual or case-by-case basis.
Level 2 Repeatable (active)	• The ITSM process generally follows a regular pattern. • Processes have developed to a stage where different people undertaking the same task follow similar procedures. • There is limited formal training or communication of standard procedures and most responsibility is left to the individual. • There is a high degree of reliance on the knowledge of individuals and errors are likely as a result.
Level 3 Defined (pro-active)	• The ITSM process is standardised & followed. • ITSM processes have been standardised, documented and communicated through formal training. • Documented ITSM processes and actual practices are general consistent although some variations may still occur. • The ITSM processes themselves are not sophisticated. • A central location has been established to maintain all available ITSM process documentation and supporting materials.
Level 4 Managed (pre-emptive)	• The ITSM process is monitored and measured; best practices are followed & automated. ITSM process performance and compliance is monitored and measured and actions taken where processes appear not to be working effectively. • ITSM processes are under constant improvement and have been refined to a level of best practice. • Benchmarking with other organisations and industry best practice is used to drive improvement. • ITSM tools are in place to automate workflow and improve quality and effectiveness, making the enterprise quick to adapt.

Level 5 Sustained (sustained performance >1 year)	• The ITSM processes, training and protocols have been followed at Level 4 continuously for more than 12 months.

2. Process Characteristics: To inform the overall maturity rating, the following process characteristics should be adopted:

Characteristic	Assessment Question
Documentation	How effectively is the ITSM process documented and maintained?
Consistency	How consistently is the ITSM process performed across individuals, teams and the Contractor?
Continual Improvement	To what extent is the ITSM process subject to continual improvement?
Customer Alignment & Value	How well is the ITSM process aligned to stakeholder and business needs and delivers valuable outcomes?
Measurement	How is performance of the ITSM process measured?
Tools	To what extent are tools used to support the effective and efficient performance of the ITSM process?
People (Org/Roles/Skills)	To what extent are the role requirements, skills and people capabilities defined and managed for the ITSM process?
End-to-End Integration	To what extent is the ITSM process deployed across multiple suppliers and services?
Integration -process integration	How well are the inter-process relationships implemented?

3 Maturity characteristics: To inform the overall maturity rating, the following process maturity characteristics should be adopted:

DOCUMENTATION	
How effectively is the process documented and maintained?	
0	There is no process documentation.
1	There are few, if any, documented procedures. Quality of documentation is poor.
2	Some processes or procedures exist but may not be fully documented. Documentation is not maintained or up to date.
3	Process is documented to a common standard; Process is unsophisticated; some shortfalls against recognised good practice. Important documents are version-numbered and changes are tracked. Documentation is maintained in a central location;
4	Process documentation is complete with policy, purpose, objectives, procedures, roles and metrics; All the required underpinning procedures are included. The process activities are aligned with recognised good practice. Documentation is protected from unauthorized change, centrally stored and backed up. Process documentation is regularly reviewed and updated (at least every 6-12 months)
5	Process has been fully documented and maintained for >12 months.

CONSISTENCY	
How consistently is the process performed across individuals, teams and the Organisation?	
0	There is no process in place
1	Performance of the activities varies according to who undertakes them. Many local procedures & variations. Documented process is not followed.
2	Procedures are usually followed but vary from person to person and team to team. Performance is becoming more consistent but is still variable. Some consistency emerging across teams;
3	Activities are carried out with a reasonable degree of consistency across the Organisation and in line with the documented process; Mistakes and failures to follow procedure are the exception. Variations between people and teams performing the activities are minimal; Outcomes are increasingly predictable and usually meet stakeholder needs; Activities are subject to planning and rarely taken on an ad hoc or unplanned basis;
4	The process or function and the associated activities are robust and rarely fail to perform as planned; Activities are performed consistently and reliably across all areas of the

CONSISTENCY	
	Organisation in which they are used. Exceptions are rare and quickly addressed; Outcomes are predictable regardless of who performs the activity; Compliance to the process and procedures is regularly checked against documented procedures by independent assessment or audit.
5	Process is institutionalised and has been sustained at level 4 for >12 months

CONTINUAL IMPROVEMENT	
To what extent is the process subject to Continual improvement?	
0	There is no process in place.
1	There is no formal procedure for making improvements.
2	Improvements are made ad-hoc on the initiative of individuals.
3	Warnings, non-compliances and variations are actively used as a source of continual service improvement (CSI); When errors are made, these are often recognized and are starting to be investigated to improve performance and reduce subsequent errors.
4	Improvements are pro-actively identified, prioritized and implemented; Regular process reviews are completed by the process owner and reviewed with stakeholders to validate continued effectiveness; Redundant or sub-optimized procedures are identified and removed; Improvements are introduced across the entire Organisation to maintain operational consistency; Performance data and stakeholder feedback are retained and analysed for trends and improvement potential;
5	Continual improvement at level 4 has been sustained for > 12 months.

CUSTOMER ALIGNMENT	
How well is the process aligned to stakeholder and business needs and delivers valuable outcomes?	
0	There is no process in place
1	Activities have a technical rather than customer or service focus; No stakeholder feedback is gathered or sought;
2	Some stakeholder feedback is provided and major issues are responded to on an ad hoc basis.

CUSTOMER ALIGNMENT	
	Improvements are focused on the activities rather than the stakeholder outcomes.
3	Feedback from stakeholders is actively sought and acted on. The internal (technical) and external (customer) focus is balanced;
4	The focus is customer and service outcomes. There is regular measurement and review of process and function effectiveness from the customer perspective;
5	Alignment to customer outcomes has been sustained for >12 months.

MEASURES	
How is performance of the process measured?	
0	There is no process in place.
1	Few, if any, records are kept of performance. Performance of the activities is subject to no, or only basic, measures such as volume and failure rate.
2	Goals and objectives are defined; Some aspects of process performance is measured and reported to at least internal stakeholders.
3	Process performance is measured using a range of metrics; Process performance is reported to both internal and external stakeholders; Metrics are fully documented
4	Process performance and activities are continuously measured and monitored; Metrics and measurements are used to assess process performance against agreed process targets and objectives; Measures are used to drive Continual improvement; Processes, procedures and functions are regularly audited for efficiency and effectiveness.
5	Measurement has been sustained for >12 months

TOOLS
To what extent are tools used to support the effective and efficient performance of the process?

TOOLS	
0	There is no process in place
1	There is little, or no, automation or use of tools or templates for any activities.
2	Some automation is starting to be used to improve efficiency; Some basic tools & templates in use; There is a lot of manual intervention;
3	At least some of the activities are automated (mostly routine activities) and supported by tools; Standard templates are defined to support process activities.
4	Most activities that can be automated are automated; Thresholds are established that generate warning alerts if a threshold is reached so that action can be taken before services are affected. Process is fully supported by tools & templates; Tools help to enforce process adherence.
5	Tools and automation have been in use for >12 months

PEOPLE	
To what extent are the role requirements, skills and people capabilities defined and managed for this process?	
0	There is no process in place.
1	There is no definition of process or functional roles; resources are not in place
2	Roles are recognized, even if they are not formally defined or fully resourced; People performing the role receive basic, 'on the job' training when they join, but little, if any, thereafter; Knowledge is shared informally between team members; there is high degree of reliance on local experts and individual abilities.
3	The activities are appropriately resourced, although occasionally, may be inadequate. Roles are formally recognized, defined and assigned. People carrying out the activities have the skills, experience, competence and knowledge to perform their role; People performing the role receive both initial and some ongoing training. Training is formalised.
4	Refresher training and updates are given in advance of a procedure or activity changing. There is a clear and documented definition of authority levels for each role. People skills are assessed and validated against changing requirements; Skills matrices or their equivalent are used to validate people's capabilities. Staff hold recognised accreditation for skills &

PEOPLE	
	knowledge
5	Skill levels are at the level of marketing leading practice Industry acknowledged expertise; contributing to thought leadership

END TO END INTEGRATION	
To what extent is the process deployed across multiple suppliers and services?	
0	There is no process in place
1	Different processes and procedures are followed for different suppliers & services;
2	This process is used to manage a limited number of suppliers or services in a consistent way;
3	The process is used consistently across all the in scope Service and Suppliers; A limited number of services are being managed end to end by this process.
4	Activities are performed seamlessly across functional interfaces both internally and externally; All services & suppliers subject to the same process. Measures, roles and procedures span the entire supply chain to include inter-related and inter-dependent internal and third-party relationships.
5	Process is used to manage end to end services for more than 12 months.

PROCESS INTEGRATION	
How well are the inter-process relationships implemented?	
0	There is no process in place.
1	There is no recognition of any inter-process relationships.
2	The relationships between this process and other processes are recognised (documented at least in part).
3	Inter-process relationships and dependencies are fully documented and have been partially established;
4	Inter-process relationships are fully established; Process and procedural interfaces and dependencies and tested for compliance;

PROCESS INTEGRATION	
	Process activities and responsibilities that span more than one team are subject to operational level agreements;
5	Process is used to managed end to end services for more than 12 months.

APPENDIX 2

ITIL Requirements

CONTENTS

Clause Heading **Page**

1 REQUIREMENTS OF ALL ITSM PROCESSES AND FUNCTIONS 2

2 SERVICE LIFECYCLE MANAGEMENT 3

3 SERVICE STRATEGY 20

4 SERVICE DESIGN 26

5 SERVICE CHANGE 37

6 SERVICE OPERATION 58

7 CONTINUAL SERVICE IMPROVEMENT 70

1 REQUIREMENTS OF ALL ITSM PROCESSES AND FUNCTIONS

1.1 For each ITSM process and function, the Contractor shall:

(a) for each non-compliance or repeat non-compliance to the Service Operation Manual, inform the Authority of all non-compliance and resolve such non-compliance with the aim of avoiding further non-compliance;

(b) ensure that roles and responsibilities across all processes and functions are clearly articulated (for example, through the use of a RACI matrix);

(c) provide comprehensive reporting across all ITSM process areas. By way of indicative example for all other process areas, the ITIL process of 'Incident Management', this shall include as a minimum the following:

(i) the time to resolve (being the number of minutes/hours/days that passed from when the incident was initially reported to its resolution);

(ii) first-time resolution rate;

(iii) compliance ratio to third party supplier service level agreements;

(iv) number of active Incidents;

(v) re-categorised Incidents;

(vi) re-open rate;

(vii) Incidents by End User role and type;

(viii) Incidents not initiated via self-service;

(ix) Incidents with associated problems;

(x) Incidents which have been escalated under 'Incident Management' process;

(xi) Incidents resolved remotely;

(xii) Incidents with no known resolution;

(xiii) ticket volume; and

(xiv) End User satisfaction;

(j) unless otherwise specified in an individual Service Requirement, outputs of reports and plans can be combined to a single reporting pack, where the reporting period and delivery expectation are consistent;

(k) unless otherwise specified in an individual Requirement, all reports contained in this Schedule shall be produced and made available to the Authority within 5 Working Days of the beginning of each Service Period and have metrics for the previous Service Period as well as prior 12 months to allow for trend analysis; and

(l) record and, if requested in accordance with Schedule 8.4 (Reports and Records Provisions), make available to the Authority such Data relating to the ITSM process and function, including (but not limited to):

(i) all ITSM tooling and metrics, including monitoring, alerting, performance, capacity management tools (service metrics required in a dynamic dashboard view, where the Authority expects to have flexibility in determining which metrics need to be reported on);

(ii) asset, inventory and Configuration Management Database (CMDB);

(iii) Incident and Problem management system; and

(iv) all test plans, test scripts and test results.

2 SERVICE LIFECYCLE MANAGEMENT

2.1 The Contractor acknowledges and understands that the purpose of ITIL process of 'Service Lifecycle Management' is to provide the tools and holistic mechanisms to coordinate and control the services and processes throughout the Service Lifecycle to manage the full lifecycle of services and contribute to the management and delivery of end-to-end services.

Toolset used for ICT Service Lifecycle Management

2.2 The Contractor acknowledges and understands that access to and management of information is a core requirement in any process management role and having an integrated ITSM toolset provides the Contractor a common interface for information on any given Service Event and to ensure the management of such events, to a successful conclusion, is available, visible, reportable and auditable from a single source.

2.3 The Contractor shall provide and maintain an ITSM toolset, access, and mechanisms to coordinate and monitor the provision and adherence to the ITSM processes and functions, which shall:

(a) be an industry recognised ITSM toolset which is readily available in the market place and which does not require specialist proprietary knowledge in its use and operation;

(b) provide, maintain and make available to the Authority (via the automated electronic ITSM toolset used for the management of the Service Events across the Service Lifecycle) for the following processes:

(i) Service Desk operation;

(ii) management of Incidents;

(iii) management of Problems;

(iv) management of the Change Control Procedure;

(v) management of Updates;

(vi) the ITIL process of 'Knowledge Management';

(vii) the ITIL process of 'Request Fulfilment'; and

(viii) the ITIL process of 'Service Asset and Configuration Management';

(c) provide a roadmap for how integration across systems management and service management toolsets will be achieved.

(d) have standard interfaces that provide the ITSM processes and functions and which can support a wide range of ICT functions without manual intervention, including (but not limited to):

(i) End User requirements capture;

(ii) project and programme management;

(iii) enterprise resource planning and management;

(iv) solution testing; and

(v) architecture management;

(e) define and make available to the Authority, the ITSM toolset's integration standards for the following architecture domains:

(i) process;

(ii) data;

(iii) application; and

(iv) infrastructure;

(f) be capable of:

(i) logging and tracking Incidents;

(ii) logging and tracking Service Requests;

(iii) providing real-time service performance status information;

(iv) providing End User help and frequently asked questions, with the facility for an End User facing knowledge base; and

(v) managing and presenting service performance reporting; and

(g) be compliant with and endorsed by the ITIL 'Software Scheme'.

Architecture Management

2.4 The Contractor acknowledges and understands that:

(a) the purpose of the ITIL process of 'Enterprise Architecture Management' is to: support the translation of the Authority's business vision and strategies into effective enterprise change; and to ensure the continuing alignment of IT Services provision to the Authority's business objectives;

(b) the purpose of the ITIL process of 'Solution Architecture Management' is to: support the delivery of specific change projects; to review architecture decisions and migration plans to identify efficiencies and advance standardisation; to ensure the solutions align to the architecture and technology principles, policies, standards and reference models defined by the ITIL process of 'Enterprise Architecture Management'; and capture and manage exceptions; and

(c) the purpose of the ITIL process of 'Existing Estate Architecture Management' is to: provide an up to date, consistent baseline of information about the provision of the end-to-end services; to contribute to the integrated change planning process from demand to delivery; and to facilitate alignment of the Existing Estate Architecture with Authority business objectives and operating models. For the avoidance of doubt, the use of the term Existing Estate Architecture is used in place of the standard term "Deployed Estate Architecture" to avoid confusion with the Authority's usage of 'Deployed' in the context of a mobilisation of the armed forces.

2.5 The Contractor shall provide 'Enterprise Architecture Management', 'Solution Architecture Management' and 'Existing Estate Architecture Management' which shall include:

(a) architecture rules, in respect of the creation and maintenance of architecture and technology principles, policies, standards and reference models;

(b) architecture specifications;

(c) improvement planning, including details of opportunities, solutions, and migration;

(d) realisation, including acquisition and implementation governance;

(e) architecture governance, in respect of architecture change management and requirements management;

(f) enforcement of standards and policies; and

(g) architecture compliance and alignment monitoring.

2.6 The Contractor shall:

(a) at the request of the Authority, participate in architecturally significant forums (for example, cross-Government technology forums and planning forums);

(b) at the request of the Authority, provide information, resources and advice to assist the Authority in undertaking:

(i) the development and agreement of changes to architecture rules (architecture and technology principles, policies, standards and reference models); and

(ii) the development and agreement of changes to the Authority's 'Enterprise Architecture Management' and architecture compliance policies, processes, and procedures;

(c) at the request of the Authority, co-ordinate 'Enterprise Architecture Management' activities which includes, as a minimum:

(i) ensuring information required by stakeholders (being those parties involved in the processes) is available in a timely and intelligible fashion, fit for purpose of the process involved;

(ii) ensuring that stakeholders (being those parties involved in the processes) are co-ordinated appropriately (for example, being notified in advance and the relevant decision bodies being convened) and resource and/or availability constraints are noted and any implications are assessed;

(iii) alerting appropriate Authority stakeholders (being those Authority staff involved in the process) with process issues (for example, backlog and bottlenecks);

(iv) ensuring stakeholders (being those parties involved in the processes) are clear on the decisions required, criteria by which they are to be made and the information needed to enable them;

(v) ensuring that Enterprise Architecture Governance is exercised at each stage of the process and is backed by authorisation to proceed in the process;

(vi) providing continuity and integrity across all process inputs and outputs to form a coherent and integrated set of Enterprise Architecture Governance materials, with known and defined risk and timescales attributes;

(vii) ensuring the architectures and technology estates defined during the 'Strategy', 'Design' and 'Transition' processes are accurately mapped to

related plans (for example, as future snapshots of proposed Architectures and Estates are mapped to Portfolio, Programme and Project plans);

(d) make available, via the Service Catalogue as a defined capability, SQEP enterprise and solution architecture resources to be requested by the Authority;

(e) ensure that changes and improvements to Services, Service Design artefacts, innovation proposals, and other solutions developed by the Contractor are:

(i) developed in alignment with the Authority's architecture rules (architecture and technology principles, policies, standards and reference models, Standards and Principles); and

(ii) subject to appropriate solution implementation governance as defined in the Authority's Architecture Compliance policies, processes and procedures;

and provide:

(iii) project design processes that create and use design materials such as logical or physical Enterprise Architecture, programme/project architecture, technical domain architecture;

(iv) identify non-compliant / exception aspects of project design, and raise these with the Authority for approval or remedial work; and

(v) raise architectural exceptions to the Authority for approval;

(f) assist the Authority to:

(i) undertake a compliance assessment of proposed changes and improvements to Services, new Services, Service Design artefacts, innovation proposals, and other solutions; and

(ii) assess compliance against the Authority's architecture rules (architecture and technology principles, policies, standards and reference models), and impact to the Existing Estate Architecture;

(g) define a portfolio of services which form 'Existing Estate Architecture Management', which shall enable the Authority and the Contractor to:

(i) determine the state of the Existing Estate Architecture in terms of the extent to which it meets the Authority's architecture rules (architecture and technology principles, policies, standards, and reference models);

(ii) access data about the Existing Estate Architecture to support Enterprise Architecture Governance processes (such as strategy and roadmap development and portfolio management); and

(iii) access data about the Existing Estate Architecture to support Solution Architecture Governance processes (such as solution design and change impact assessment);

(h) data governance, data reference models and data architecture requirements to align to those set out in Schedule 2.10 (MI & Data) and Annex H (MIL MIT & Data);

(i) within the ITIL 'Existing Estate Architecture Management' maintains and provides all necessary data about the architecture currently deployed in support of the Services to allow compliance and alignment to be assessed, including (but not limited to):

(i) definition of policies, processes and procedures for managing all necessary data about the Existing Estate Architecture;

(ii) provision of high level and low level architectural and solution design documentation relating to the Services;

(iii) definition of a data model and reference model for structuring data held about the Existing Estate Architecture;

(iv) sourcing of data from the ITSM toolset and other relevant sources; and

(v) deployment of a tool for maintaining the Existing Estate Architecture data;

(j) manage the ITIL 'Existing Estate Architecture Management', including (but not limited to) elements for definitions of processes, roles, RACI matrices, and work products which shall be made available to Authority;

(k) ensure that:

(i) policies, processes and procedures, defined in relation to the ITIL process of 'Existing Estate Architecture Management' integrate with the Authority's 'Enterprise Architecture Management' and architecture compliance processes; and

(ii) data models and reference models defined are aligned with the Authority's data models and architecture reference models;

(l) deploy the ITIL process of 'Existing Estate Architecture Management', including (but not limited to):

(i) provision of high level and low level architectural and solution design documentation relating to the Services; and

(ii) adoption of the associated data model and reference model, in support of the Services;

(m) ensure that the ITIL process of 'Existing Estate Architecture Management' and its content are effectively communicated to the Authority;

(n) each Quarter, assess the compliance of Existing Estate Architecture against the Authority's architecture and technology principles, policies, standards, and reference models (the content of such an assessment to be agreed with the Authority);

(o) update and maintain all architecture and design artefacts for the Existing Estate Architecture from Operational Service Commencement Date, so that they reflect the existing technology estate implementation; and

(p) ensure that an impact assessment against the Authority's Existing Estate Architecture is carried out on Service assets and associated configuration items within the Service Catalogue which require replacement, update or retirement in line with the Change Control Procedure.

Architecture Management Office

2.7 The Contractor acknowledges and understands that an effective Architecture Management Office (AMO) is necessary to provide robust design control and ensure all Change is managed in accordance with the required standards and principles, roadmaps, methods, and strategic change plans; the Contractor provisioned AMO must work in collaboration with the Authority Design Assurance function, to enable a joint decision-making and governance function that will be managed through a Joint Architecture Governance framework, including (but not limited to) the Joint Architecture Board; the AMO will be responsible for creating and maintaining the service and solution design artefacts but must work closely with the Authority Design Assurance to ensure that the Authority domain knowledge and expertise is meaningfully engaged and that the Service Strategy is an Authority owned outcome of transparent and collaborative working; and the AMO must be a central function of the Service provision and be at the centre of all Service Change and Service Design activity, to ensure that an enterprise wide architectural view is collaboratively maintained and enforced.

2.8 The Contractor shall:

(m) from Operational Service Commencement, establish and maintain a Joint Architecture Governance framework which shall:

(i) define the engagement model for the AMO and Authority Design Assurance, which clearly establishes the roles, responsibilities, ownership for the Contractor and Authority, and setting out the resources and the capabilities required;

(ii) define a practical engagement pattern for the collaborative working of the AMO and the Authority Design Assurance teams;

(iii) provide and maintain a design approval process with clear identification of roles and responsibilities of the Parties;

(iv) provide and maintain usable governance material and activities;

(v) provide a mechanism for the formal acceptance and approval of architecture through consensus and authorised publication;

(vi) provide a fundamental control mechanism for ensuring the effective implementation of the architecture;

(vii) provide and maintain a link between the implementation of the architecture, the architectural strategy, and objectives embodied in the enterprise architecture and the strategic objectives of the business; and

(viii) identifying divergence from the architecture and planning activities for realignment through dispensations or policy updates;

(n) from Operational Service Commencement, establish and maintain a mature AMO to do the following:

(i) govern all elements of the Services, provide all required architectural artefacts for access and use by the Authority;

(ii) ensure that business, data, application, security, and technology architectures are collaboratively developed with the Authority;

(iii) lead the engagement with the Security Management functions (as set out in Schedule 2.4 (Security Management)) to ensure that all aspects of security architecture and design is a conjoined activity;

(o) provide and maintain TOR and/or RACI matrices for all roles within the AMO;

(p) provide a consistent cadre of SME's and Architects across the architecture domains (business, security, data, tech/apps), with proven experience of operating in such roles in other similar organisations and scale;

(q) provide and maintain the products and/or artefacts that will be needed to ensure the strategic initiatives are turned into meaningful change, including (but not limited to) roadmaps, standards, impact assessments and use of EA modelling tools (which shall be ArchiMate compliant);

(r) create and maintain a set of technology standards, that is an accurate reflection of all standards and principles that have been agreed;

(s) at Operational Services Commencement Date, provide a detailed plan for Authority approval, identifying the activities and deliverables that will support the introduction of the AMO;

(i) in-scope elements, including (but not limited to) those set out in this Agreement; and

(ii) details of Deliverable, including (but not limited to) the benefits, dependencies, risks, costs, timescales, outputs, reporting Performance Indicator metrics to be provided and the targets to be met;

(t) ensure that Authority Design Assurance resources can work alongside the Contractor AMO team in a shared space when required;

(u) engage via the Authority with central Authority policy creation organisations to capture requirements, including (but not limited to) supporting the Modernising Defence Programme (or its successor programme) with both project control and technical resources and policy simplification will take place until the completion of the Transformation process. This will need to be supported by the AMO;

(v) provide architecture governance and architectural advice, owning and driving the process of translating business vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future state and enables its evolution;

(w) create, manage and fully engage with a Joint Architecture Board, alongside Authority Design Assurance staff, which is responsible, and accountable, for achieving the following goals:

(i) consistency between sub-architectures;

(ii) identifying re-usable components;

(iii) flexibility of enterprise architecture to meet changing business needs;

(iv) flexibility of enterprise architecture to leverage new technologies;

(v) enforcement of Architecture compliance to the applicable standards, guidelines and principles;

(vi) improving the maturity level of architecture discipline within the Contractor and Authority;

(vii) ensuring that the discipline of architecture-based development is adopted;

(viii) providing the basis for all decision-making with regard to changes to the architectures; and

(ix) supporting a visible escalation capability for out-of-bounds decisions.

(x) ensure that the Joint Architecture Board has the further responsibilities from a Service Operation perspective, including (but not limited to):

(i) all aspects of monitoring and control of the Architecture aspects of the Agreement;

(ii) meeting on a regular basis;

(iii) ensuring the effective and consistent management and implementation of the architectures;

(iv) resolving ambiguities, issues, or conflicts that have been escalated;

(v) providing advice, guidance, and information;

(vi) ensuring compliance with the architectures, and granting dispensations that are in keeping with the technology strategy, objectives, standards and guidelines;

(vii) considering policy changes where similar dispensations are requested and granted (for example, through a new Service Requirement);

(viii) ensuring that all information relevant to the implementation of the Architecture aspects of the Agreement is published under controlled conditions and made available to authorised parties; and

(ix) validation of reported Performance Indicators and cost savings;

(y) from Operational Services Commencement Date, provide a detailed plan for Authority approval, identifying the activities and deliverables that will support the introduction of the Joint Architecture Governance framework and Joint Architecture Board:

(i) in scope elements, including (but not limited to) the Obligations set out in this Schedule; and

(ii) details of Deliverables, including (but not limited to) the benefits, dependencies, risks, costs, timescales, outputs, reporting Performance Indicator metrics to be provided and the targets to be met.

(z) provision and utilise an Enterprise Architecture modelling tool (which is to become the primary tool used by the AMO) in support of the AMO capability for use by the Authority and Contractor;

(aa) adopt and use an Enterprise Architecture modelling tool to support the description, analysis and visualisation of architecture within and across business domains. This must be an ArchiMate modelling language certified tool;

(bb) ensure AMO and Joint Architecture Board artefacts which need to be produced, are maintained and accessible to the Authority, including (but not limited to) models, roadmaps, standards, and policies;

(cc) agreed changes to artefacts should be made available to the Authority within 5 Working Days, unless otherwise agreed with the Authority;

(dd) throughout the Term, ensure that the Enterprise Architecture modelling tool is made available to up to 20 Authority staff, as a read-only capability;

(ee) create and maintain a sustainability plan assessing all ICT used to deliver the Services, covering areas including (but not limited to):

(i) energy;

(ii) product weight;

(iii) packaging;

(iv) hazardous substances; and

(v) recyclability (to include which element is recyclable, method of recycling, those not recyclable, and method of disposal); and

(ff) provide and maintain Roadmaps for all Services that utilise ICT covering the period of the Term +2 years;

Supporting the Authority Role

2.9 The Contractor acknowledges and understands that the purpose of these requirements is to support the Authority in its changing role and ensure that the Authority has explored all options in deciding the most appropriate ICT function to enable the successful implementation and operation of its Target Operating Model.

2.10 The Contractor shall:

(a) make proactive contribution to the creation of Service Strategy and comply with Authority strategy generation and implementation processes as they evolve;

(b) provide information, resources and advice to assist the Authority in undertaking the following:

(i) developing its vision for Services;

(ii) develop specific strategies for ICT capabilities as requested by the Authority based on Authority business requirements;

(iii) undertake assessments of alternative options developed by the Authority;

(iv) provide input, guidance and analysis around external factors (political, economic, social, technology – 'PEST', and strengths, weaknesses, opportunities, threats – 'SWOT') as requested by the Authority; and

(v) undertake any relevant market analysis to identify opportunities and innovations that shall support the Authority in achieving its strategic objectives;

(c) support the Authority in the activities required to perform assessments on the current state of Services in delivering to the Authority's strategic objectives for Services, including (but not limited to) undertaking:

(i) target state definition for Services;

(ii) gap analysis between current and target state;

(iii) option analysis and estimation of work required to achieve the target state for a given Service and/or end-to-end Services; and

(iv) developing roadmaps for a Service and/or end-to-end Services;

(d) provide a portfolio of Services that enable the Authority to delegate or outsource a significant amount of the mechanics and analysis involved in managing Enterprise Architecture artefacts, including (but not limited to):

(i) vision and strategy;

(ii) architecture rules management (such as principles and technology policy);

(iii) architecture specification (for business, information/data systems, and ICT);

(iv) improvement planning (for opportunities, solutions, migration, and transformation);

(v) realisation (including acquisition and implementation governance);

(vi) architecture governance (for architecture change management and requirements management); and

(vii) architecture performance monitoring and management;

(e) on request, provide the Authority with a model of the future-state architecture based on the future-state project pipeline;

(f) with reference to authorised End Users and the granting of access to resources in support of the ITSM lifecycle, provide an approach to managing other Contractors and the Authority personnel in granting the appropriate access to resources in support to requesting, consuming and supporting the Services;

(g) when reporting to the Programme Board in accordance with Clause 8.1 on the identification of new or potential improvements to the Service in the context of 'Architecture Management', ensure the reports contain (but not be limited to):

(i) 'Rough Order of Magnitude' estimates in line with and supporting the requirements of the Authority's integrated ICT lifecycle:

(ii) advice and guidance to the Authority on options and alternative approaches to service solutions to meeting business requirements;

(iii) details on how such improvements will support the Authority in achieving its business requirements; and

(iv) estimates of the level of complexity, strategic alignment, resource requirements, costs, and timescales;

(h) report on demand trends for the Services, with the purpose of identifying and reporting risks inherent in demand forecasts and capability to meet demand;

(i) support the Authority in minimising its costs while maximising the value it receives from the Services, including (but not limited to):

(i) developing 'Demand Management' models;

(ii) making recommendations to reduce demands on Services;

(iii) making recommendations to existing capacity plans to reflect how Services will be affected by demand projections (including the steps needed to meet demand projections);

(iv) making available to the Authority stakeholders (being those parties involved in the process) the mechanisms in place to control demand for Services; and

(v) making recommendations to the Authority for improvements of the mechanisms to control and meet current and forecast demand for Services; and

(j) when requested by the Authority, work in consultation and agreement with the Authority on an ITIL process, to encourage End Users to make the most efficient use of the Services available;

2.11 The Contractor shall provide support to the Authority with the development of Authority Requirements through:

(a) supporting the Authority in establishing the required business capability, functionality and non-functionality, including (but not limited to):

(i) analysis of statements of business capability and associated requirements to establish whether they are necessary and sufficient;

(ii) analyse requirements to balance stakeholder needs and constraints; and

(iii) validate requirements to ensure resulting products and services shall perform as intended both in terms of meeting stated business capabilities and operating in the Technical Infrastructure;

(b) providing support, guidance and management in establishing and maintaining guidelines in the determination of option appraisals for proposed solutions to business requirements, with the purpose of ensuring all options are subjected to a formal evaluation process;

(c) establishing and maintaining criteria for evaluating service option alternatives and relative ranking criteria;

(d) providing and maintaining operational procedures for planning and performing the requirements development process (ensuring that they are aligned to the Authority's policies and standards for the development of solution and service requirements) which demonstrate the following characteristics:

(i) consistent and repeatable;

(ii) conform to industry best practice;

(iii) be open and transparent to the Authority;

(iv) be achievable within planned timeframes, budgets and resources;

(v) align to the Authority's ways of working; and

(vi) be optimised for efficiency;

(e) ensuring that appropriate resources for performing the work in developing approved products and providing the services for the requirements development process are in place and that the following is carried out as required and in agreement with the Authority:

(i) assign responsibility and Authority for performing the process, developing the work products and providing the services of the requirements development process;

(ii) provide training to the relevant Authority staff, performing or supporting the requirements development process as needed;

(iii) place designated work products of the requirements development process under appropriate levels of configuration management; and

(iv) identify and involve the relevant stakeholders of the requirements development process as planned;

(f) supporting in the monitoring and control of the requirements development process against agreed plans and take appropriate corrective action to mitigate poor performance;

(g) supporting in the review of the activities, status and results of the requirements development process with nominated Authority staff and work to resolve issues;

(h) ensuring efficient management of the granting of authorisation to End Users and the management of lists of End Users;

(i) providing the Authority with immediate read-only access to all service information, including (but not limited to):

(i) all Contractor System and ITSM tooling, including monitoring, alerting, performance, capacity management tools;

(ii) asset inventory and configuration management database;

(iii) Incident and Problem management system; and

(iv) all test plans and test results, through the chosen test tools;

(j) ensuring, where Contractor teams are located at Authority Premises, hot desking allowances are made to allow Authority personnel to be able to co-locate in work areas, to help facilitate collaborative working;

(k) ensuring, where Contractor teams are located off-site, an alternative disparate staffing enabling mechanism is in place to ensure the Authority teams can work closely with Contractor and the supplier teams;

(l) implement, deliver and maintain a configurable and dynamic dashboard view capability of all metrics supporting the ITSM delivery across all elements of the Services;

(m) deliver and maintain service reporting of Performance Indicators via a dynamic dashboard view and the Authority expects to have flexibility in determining which metrics need to be reported on;

(n) provide dynamic dashboards for service metrics, including (but not limited to) capacity, performance, usage, incident, problem management, changes planned/completed, service health and the Authority requires mature reporting that is dynamic and comprehensive; and

(o) provide a dashboarding and service reporting capability that meets the Authority expectation to agree all the metrics that will be initially made available, but these will not be the sole and static expectation, as this will advance as ITSM Matures.

Application Performance Monitoring

2.12 The Contractor acknowledges and understands that the Authority requires the ability to monitor the performance of all Applications and their component elements which are used in the delivery and consumption of the Services and that:

(a) such application performance monitoring will need to accommodate all stages of the Application functional lifecycle;

(b) the Contractor is responsible for maintaining an appropriate level of performance and availability for all business applications by continuously monitoring and measuring their performance and promptly identifying and reporting to the Authority any potential issue.

(c) the Authority requires access to these application performance monitoring tools to help realise the following benefits:

(i) understand the real end user experience of using an Application;

(ii) anticipate future bottlenecks and pro-actively manage availability and capacity of Business Applications;

(iii) identify trends of business applications usage to possibly offer improvements in both performance and availability of the application; and

(iv) detect application performance degradation early and propose actions to prevent potential service disruption.

2.13 The Contractor shall:

(a) provide an application performance monitoring service which shall:

(i) support other processes across the Service delivery lifecycle, including (but not limited to):

(A) 'Availability Management';

(B) 'Capacity Management'; and

(C) 'Problem Management';

(ii) provide an application performance monitoring service that offers the following characteristics:

(A) the taking of measurements must be passive in nature and must not have any impact on the performance of either the Business Application being measured or the infrastructure it is accessed through, unless otherwise agreed with the Authority;

(B) centrally managed and controlled using automated orchestration tools; and

(C) integrates and makes use of the metrics and measurements available for the Technology Infrastructure layer performance toolsets, to establish full service performance monitoring capability;

(iii) measure the end-to-end performance of the full suite of Applications (unless agreed with the Authority);

(iv) gather and aggregate data to a functional Business Processes level of granularity, to allow the Authority to identify performance levels across specific function areas;

(v) enables the gathering of performance metrics and in doing so:

(A) is configurable easily and rapidly for applications in problem determination;

(B) is platform and product agnostic and so can be deployed on any infrastructure and monitor any Application;

(C) is scalable to be able to monitor more Applications as required;

(D) monitors multiple transactions per Application;

(E) monitors the time for login from any station by any end user;

(F) integrates and make use of any Application inherent performance monitoring capability;

(G) includes configurable thresholds and can issue alerts centrally where a criterion being measured crosses the threshold; and

(H) captures performance from all user / locations / applications where each Application can be accessed to ensure full coverage of all components involved in the delivery of the Application;

(b) manage the collection and recording of all Application performance measurements and information in support of the application performance monitoring service in a central repository and retained thereafter and in line with Schedule 2.6 (Data);

(c) manage the baselining of the 'Applications for Performance' measurement;

(d) ensure, for all Applications to be baselined, that their Performance is measured for an initial period of 3 months to provide an initial baseline against which future metrics will be measured;

(e) provide a report to the Authority, after the initial period of 3 months and for each Application to be monitored, detailing the Performance observed during the baselining and make recommendations to the Authority on the service thresholds and Performance Indicators to be set on each Application to be measured;

(f) provide an Application Performance monthly report to the Authority, which clearly provides performance metrics which allow the Authority to accurately assess the End User experience of using the Applications for specific business functions;

(g) when requested by the Authority to extend the application performance monitoring service, plan and coordinate for the baselining and subsequent performance monitoring of that additional Application; and

(h) upon request from the Authority, plan for and implement a fast-track monitoring service for any specific Application and include this specific Application in the list of the application performance monitoring service for a limited time (as determined by the Authority) which may include (but is not limited to):

(i) End User experience monitoring;

(ii) problem determination;

(iii) usage analysis and development of trends; and

(iv) early life measurement for either new applications or following a New Release.

3 SERVICE STRATEGY

Service Strategy stage

3.1 The Contractor acknowledges and understands the purpose of the ITIL 'Service Strategy' stage is to create value for the Authority by assisting in the identification, evaluation, selection and prioritisation of opportunities to develop end-to-end Services that must meet the current demands and future requirements of the Authority, whilst delivering best value. This will provide new starters as well as existing staff with a clear strategy and direction for the Services for the Term. It is expected that this will be largely influenced by the agreed Contractor solution. However, this will need to evolve as external influences and requirements develop over the course of the contract.

3.2 The Contractor shall:

(a) develop and maintain and, at each Service Period, provide to the Authority, a Service Strategy Plan; and

(b) ensure the strategic approach for the whole lifecycle will be developed to provide value to the Authority through ITSM. This should consider the service value

definition, business-case development, service assets and analysis of internal / external influences.

3.3 The Service Strategy Plan shall include (but not be limited to) how the Contractor is going to achieve the following:

(a) 'Strategy Management for IT Services';

(b) 'Demand Management';

(c) 'Financial Management for IT services';

(d) 'Service Portfolio Management'; and

(e) 'Business Relationship Management'.

Strategy Management for IT Services

3.4 The Contractor shall:

(a) have in place processes and measures for the IT Services to define and plan strategic initiatives and ensure the implementation of those initiatives.

(b) request business planning information from the Authority to highlight, for example, planned business changes/initiatives and other strategic changes that will impact requirements on this service;

Demand Management

3.5 The Contractor acknowledges and understands that the ITIL process of 'Demand Management' aims to manage the uncertainty in business demand for ICT Services and ensure the appropriate capacity of an end-to-end ICT Service is available as and when required by the Authority. Such 'Demand Management' will allow the Contractor to understand the Authority consumption requirements for ICT Services and how these vary over the Term, with the aim of ensuring the provision of an appropriate level of service to support the Authority needs. Effective 'Demand Management' will:

(a) optimise the Services to meet the patterns of business activity they support;

(b) effective management of the Service Catalogue by mapping demand to appropriate ICT Services;

(c) informs investment decisions in the management of the Services;

(d) informs resource scheduling and management;

(e) enables the ITIL process of 'Financial Management';

(f) to evaluate the true cost of ICT Services, forecast and plan future budgeting and expenditure and

(g) contains processes and measures that ensure the Authority's demands are understood, anticipated and influenced where needed.

3.6 The Contractor shall:

(a) perform activity-based analysis to identify the patterns of business activity for Services against defined business cycles to be agreed with the Authority and recorded and measured in the Service Operation Manual. Required profiles are initially expected to be hourly, daily, weekly, monthly and annually;

(b) in conjunction with the Authority, codify the patterns of business activity by establishing appropriate attributes to describe the business activity observed and its association to the consumption of Services;

(c) provide full access to all analysis to the Authority and report activity based on the Service Period and on an as required or requested by basis;

(d) manage and coordinate reporting to the Authority on the patterns of business activity by user profile, activity level for each Service Period;

(e) for each Service Period, perform forecasting activities on ICT Services to outline the pipeline and anticipate as possible the future business demand and must report such to the Authority; and

(f) make recommendations to the Authority on changes or improvements to the composition of ICT Services, including appropriate Performance Indicators (as contained in Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability).

Financial Management for IT Services

3.7 The Contractor acknowledges and understands that the ITIL process of 'Financial Management' must provide the Authority with the quantification of the value of all ICT Services provided by the Contractor and consumed by the Authority in financial terms. The 'Financial Management' service is required to ensure that the Authority only pays for the ICT Services it consumes or is obligated to pay for in line with appropriate commercial agreements. The 'Financial Management' shall help and support the Authority in being able to:

(a) improve and enhance decision making to enable the achievement of stated ICT 'run and maintain' savings;

(b) determine the size, scope and complexity of the Service Portfolio;

(c) ensures financial compliance and control;

(d) apportion charges appropriately;

(e) maintain operational control; and

(f) conduct service lifecycle investment analysis.

Service Portfolio Management

3.8 The Contractor acknowledges and understands that the ITIL process of 'Service Portfolio Management' is responsible for managing the Service and ensuring that business value is achieved across all Services provided to the Authority. Service Portfolio Management provides the overall governance in the identification, provision of, delivery and retirement of Services provided by the Contractor.

3.9 The Contractor shall:

(a) work with the Authority in providing the Service Portfolio Management and shall identify and present to the Authority suggestions for the aggregation, improvement, refresh and retirement of Services to the Authority;

(b) define and provide these services at the required level that allow the Authority to achieve its business outcomes and meet the Authority's requirements;

(c) the value of Service Portfolio Management to the Authority is demonstrated through the ability to anticipate change while maintaining traceability to the Authority's overarching ICT strategy and planning by:

(i) providing the means to characterise service investments; and

(ii) providing an essential link between business portfolio management (demand pipeline) and ICT project and programme portfolio management;

(d) produce the Service Portfolio which shall comprise:

(i) the pipeline section, which contains the services that are yet to be offered;

(ii) the service catalogue section, which contains the details of operational services; and

(iii) the retired section, which contains details of the services that are no longer offered;

(e) review and collate all Services into a Service Portfolio. The Contractor must manage the Service Portfolio and ensure that it sets out:

(i) a complete set of current Services provided;

(ii) the 'Service Pipeline' for all Services in development; and

(iii) Services currently being retired or in the process of being decommissioned;

(f) update the Service Portfolio each Quarter and make available to the Authority electronically without request; and

(g) ensure that the Service Portfolio contains the service offerings that are available from the service provider.

Risk Management

3.10 The Contractor acknowledges and understands that ITIL 'Risk Management' supports the decision-making process by being able to accurately assess risks and the associated impacts and potential benefits of actions in relation to the ability to support and deliver services. Effective Risk Management enables the identification of positive and negative risks to be analysed and a course of action to be determined based on value and impact to the Service Lifecycle, ensuring that the best possible outcome can be achieved.

3.11 The Contractor shall:

(a) align the ITIL process of 'Risk Management' with the Authority's strategic risk management approach and which shall contain the following steps across the Service Lifecycle:

(i) identification and assessment of exposure to risk and subsequent impacts;

(ii) application of appropriate controls to manage exposure and impact;

(iii) ensure communication of mitigating actions; and

(iv) management of risk is performed within a transparent, repeatable and consistent process.

(b) perform the ITIL process of 'Risk Management' in accordance with:

(i) the risk requirements as set out in Schedule 8.1 (Governance);

(ii) the security risk requirements as set out in Schedule 2.4 (Security Management); and

(iii) the Business Continuity requirements as set out in Schedule 8.6 (Business Continuity and Disaster Recovery);

(c) ensure that identification, analysis and management of risk are performed across the Service Lifecycle in accordance with the Risk Management policies and procedures;

(d) make available to the Authority the appropriate 'Risk Management' information for the purposes of ensuring that all risks are being managed appropriately and where

required, captured on the Authority's Risk Register in accordance with Schedule 8.1 (Governance);

(e) conduct proactive monitoring to identify any emergent risk to the provision of the Services;

(f) advise the Authority of any emerging risks and provide a proposal of how such emerging risks should be addressed in accordance with the current BCDR Plans and BCDR policies and procedures;

(g) organise and convene regular (quarterly at least) and emergency risk reviews to identify and recommend to the Authority appropriate measures to mitigate any risks identified; and

(h) submit to the Authority for Approval any measures identified to address any emerging risk.

Business Relationship Management

3.12 The Contractor acknowledges and understands that the ITIL process of 'Business Relationship Management' (BRM) is necessary to maintain a positive and productive working relationship between the Contractor and Authority, which is important to meeting the transformation requirements that the Authority seeks. The BRM process is to be used to establish the needs of the Authority and ensure that appropriate services are developed to meet those needs. Require processes and measures in place to ensure that a positive relationship is maintained between the Authority and Contractor, including (but not limited to):

(a) maintaining Authority Relationships to ensure that the Authority's needs are understood and maintaining the Authorities portfolio;

(b) identify Service Requirements to ensure that the Authorities desired outcome for a service is understood and documented. Use these requirements to determine if the need can be fulfilled by an existing service or whether a changed service is required;

(c) manage utilising of standard services with new End Users;

(d) plan, carry out and evaluate regular Authority satisfaction surveys;

(e) handle Authority complaints; and

(f) monitor Authority complaints.

3.13 The Contractor shall:

(a) perform the ITIL process of 'Business Relationship Management' in accordance with the Authority's Business Relationship Management and Governance requirements (as set out in Schedule 8.1 (Governance));

(b) ensure that roles and responsibilities across all processes are clearly articulated, clearly demonstrating the RACI matrices for role types which are to be updated and maintained by the Contractor throughout the Term and reviewed quarterly in consultation with the Authority;

(c) provide a detailed organisation chart (graphical and textual) in electronic format for all resources, to be updated quarterly or when significant resource churn (5 or more changes) has altered the extant chart significantly; and

(d) provide the following information annually for every role type used in connection with delivery of the Service:

(i) terms of reference (Accountabilities, Responsibilities, place in management - hierarchy);

(ii) location details; and

(iii) grade and link to rate card for Change costs.

4 SERVICE DESIGN

Service Design stage

4.1 The Contractor acknowledges and understands the purpose of the ITIL 'Service Design' stage is to ensure that the design and development of Services, both current and future, deliver value to the Authority and that the ITIL process of 'Service Design' is established that ensure the accurate design of IT Services, processes, and other aspects of the service management effort. The Contractor acknowledges and understands that the ITIL process of 'Service Design' should encompass all elements relevant to ICT service delivery, rather than focusing solely on design of the technology itself and, as such, the service design should address how a planned service solution interacts with the larger business and technical environments, service management systems required to support the service, processes which interact with the service, technology, and architecture required to support the service, and the supply chain required to support the planned service so must consider the overall Service and should be managed within the service catalogues. The ITIL 'Service Design' process shall cover how the Contractor is going to achieve:

(a) 'Design Coordination';

(b) 'Service Catalogue Management';

(c) 'Service-level Management';

(d) 'Availability Management';

(e) 'Capacity Management';

(f) 'IT Service Continuity Management';

(g) 'Security Management'; and

(h) 'Contractor Management'.

Design Coordination

4.2 The Contractor acknowledges and understands that the purpose of the ITIL process of 'Design Coordination' provides the coordination of all service design activities, processes and resources which must ensure the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics.

Availability Management

4.3 The Contractor acknowledges and understands that the purpose of the ITIL process of 'Availability Management' is to define, analyse, plan, measure and improve all aspects of the availability of IT Environment, systems and services to ensure that all ICT infrastructure, processes, tools and resources are appropriate for the agreed availability targets.

4.4 The Contractor shall:

(a) perform the ITIL process of 'Availability management in accordance with the availability and capacity management requirements as set out in Schedule 8.6 (Business Continuity and Disaster Recovery);

(b) at every Service Period, produce and issue to the Authority an 'Availability Report' in accordance with the 'Availability Management' policies, processes and procedures;

(c) ensure maintainability processes are in place to ensure the IT Services can be changes as required whilst still satisfying the Authority's business requirements;

(d) ensure availability management processes are in place to sustain IT service availability in accordance with the Authority's business requirements, for the required period of time;

(e) deliver and maintain availability testing schedule for the regular testing of all Services;

(f) provide availability requirements, which need to be accurately defined, compiling availability plans, monitoring availability, and monitoring maintenance obligations;

(g) provide reliability management processes to ensure the IT service meets the Authority's business requirements;

(h) carry out regular availability risk reviews across all services, providing a written risk review assessment and remediation report to the Authority on a Quarterly basis;

(i) provide regular availability risk analysis reports and information to the Authority, on a minimum Quarterly basis;

(j) following availability risk analysis, the Contractor must update the Authority's Risk Register in accordance with Schedule 8.1 (Governance);

(k) ensure the overall security of the service complies with all requirements including the confidentiality, integrity, and availability of Data;

(l) utilising data from capacity management process, the Availability Management function must regularly review and propose alterations necessary to meet service obligations of Authority and Contractor;

(m) work with the Authority to schedule, coordinate and manage any Service Outage in accordance with the Availability Management Policies, Processes and Procedures to minimise disruption to reflect patterns of business activity;

(n) produce, maintain and circulate to the Authority a schedule of projected Service Outage (including projected end-to-end Services Outages);

(o) ensure that the management and reporting of the service and components thereof are configured in a way that ensures all deviations in availability, reliability and maintainability of Performance Indicators are detected, recorded, actioned, and reported in accordance with the Availability Management Policies, Processes and Procedures;

(p) ensure that the management and reporting of the Services and components thereof are configured in a way that ensures the information captured can be used in planning IT Service Continuity for the Services;

(q) provide to the Authority analysis and reporting on all key elements of Service Availability in accordance with Availability Management Policies, Processes and Procedures so that it is clear where Services and components thereof are failing in the chain of delivery and where Performance Indicators for Services availability (contained in Appendix 1 of Annex M to Schedule 2.1 (Non-Functional Requirements and Service Availability) have not been achieved;

(r) gather availability data for Services and Service Components and record and maintain this data in a service availability management system;

(s) monitor and analyse the Services against the availability Performance Indicators and report these to the Authority;

(t) collect and store operational data relating to availability of the Services for the full Term (starting from Operational Service Commencement Date). The Contractor must make this data available to the Authority;

(u) ensure that measures are in place and processes established to ensure the necessary resilience/redundancy is provided;

(v) provide a Service Availability real-time measurement and reporting capability is in place that raises Alerts accordingly should user or Service Availability become lost or degraded;

(w) investigate and implement measures to improve Service Availability; and

(x) within each Service Reporting Period, conduct an impact analysis of the data on component failure and provide to the Authority the collated analysis data on component failure and proposed possible mitigation actions to avoid future degradation to the Services availability in accordance with the Service Operation Manual.

Capacity Management

4.5 The Contractor acknowledges and understands that the purpose of the ITIL process of 'Capacity Management' is to ensure that there is capacity of the Services and that resources are planned and scheduled to provide a consistent level of service that is matched to the current and future needs of the Authority.

4.6 The Contractor shall:

(a) define and agree with the Authority a list of the Data that should be gathered by the Contractor to enable well informed 'Capacity Management' decisions and:

(i) utilising automated monitoring tools, monitor such Data across all the Technical Infrastructure; and

(ii) produce detailed reporting on such Data to facilitate the Contractor in conducting Incident avoidance and resolution;

(b) notify the Authority of the Capacity thresholds to be used for the Contractor's Event and Capacity management toolset;

(c) produce, gather and collate the Capacity Reports for all services and maintain a consolidated Capacity Plan, to be made available to the Authority;

(d) provide a service (including its technology, systems architecture, services and functionality) that will be scalable to support potential extension (or reduction) into new services, or to respond to changes in Capacity or service demands in the future;

(e) update the Capacity Plan for ICT Service to reflect the Authority's quarterly business forecast provided by the Authority. Ensure that the ICT Service Capacity Plan caters for, including (but not limited to):

(i) fluctuations in business as usual capacity demand;

(ii) planned business change;

(iii) patterns of business activity;

(iv) revised or new Performance Indicators;

(v) revised or new ICT services;

(vi) ITSCM;

(vii) transition requirements;

(viii) the impact of emerging technologies within the Service Pipeline;

(ix) external changes, for example legislative changes; and

(x) software Development Life-Cycle activity;

(f) gather, record and maintain information on 'Service Capacity' across all Services in an integrated 'Capacity Management' toolset;

(g) produce a report for the Authority, covering each Application Instance, the total amount of storage, memory and processing available, the total amount of storage, memory and processing in use or allocated, and the same figures for unused or unallocated storage memory and processing. Such notification is required in order to assess options for future requirements in the remaining period until next technical refresh and cater for the 6 month lead time to make provision for additional capacity if this is the option to be pursued;

(h) analyse and report to the Authority on all key elements of 'Capacity Management' so that it is clear where there are failures to provide sufficient Capacity of ICT Services in the chain of delivery and where Performance Indicators for Capacity have not been achieved. Such analysis must include utilisation, rationalisation, performance and security measures;

(i) model the proposed Changes and consumption trends in the ICT Services to identify the Changes that need to be made to current ICT Services to ensure that the Capacity Performance Indicators continue to be achieved;

(j) produce, manage, and maintain a Capacity Model, including (but not limited to) the following activities:

(i) application sizing;

(ii) workload management;

(iii) demand management;

(iv) modelling;

(v) capacity planning;

(vi) resource management; and

(vii) performance management.

(k) coordinate the availability of appropriate resources across all services to meet the predicted changes to the ICT Services;

(l) monitor the all Services against the agreed Capacity thresholds and notify the Authority as soon as they become aware of any Capacity issue or potential Capacity issue and provide a proposal of how to address such issue;

(m) define Capacity thresholds, in agreement with the Authority, which must be configurable and able to be altered after agreement. Such to be delivered via a systemised process;

(n) manage Service Events and Capacity within the agreed Capacity Thresholds;

(o) automatically inform the Authority when growth capacity in any one of the data centres reach agreed allocation or utilisation, within 4 Working Days of becoming aware;

(p) ensure that all services are continually monitored and optimised for Capacity and increase or decrease Capacity in order to maintain the operation of the services;

(q) present to the Authority a consolidated Capacity Plan within 5 days of each Quarter in accordance with the 'Capacity Management' policies and procedures; and

(r) base any future estimates of the Capacity and demand Requirements of the Service on the following:

(i) reporting on any specific Incidents, Problems or Service Events which have been triggered by insufficient Capacity;

(ii) details of any planned upgrades or procurements for extra Capacity; and

(iii) details of any potential Capacity risks and associated mitigating actions.

IT Service Continuity Management

4.7 The Contractor acknowledges and understands that the ITIL process of 'IT Service Continuity Management' (ITSCM) manages the risks that could seriously impact the performance and availability of the Services as part of the end-to-end Services; ensures that Services can be provided in accordance with agreed Performance Indicators; supports the Authority's overall BC planning process (contained in Schedule 8.6 (Business Continue and Disaster Recovery)s by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data holdings and repositories, telecommunications, environment,

technical support and Service Desk) can be resumed within required and agreed business timescales; .and ensures that the recovery arrangements for designated Services and components thereof are aligned to identified and agreed business impacts, risks and needs. ITSCM should consider (but not be limited to) the following:

(a) prioritising the activities to be recovered by conducting a BIA;

(b) performing a risk assessment (aka risk analysis) for each of the IT services to identify the assets, threats, vulnerabilities and countermeasures for each Service;

(c) evaluating the options for recovery;

(d) producing the contingency plan; and

(e) testing, reviewing, and revising the plan on a regular basis.

4.8 The ITIL process of ITSCM shall fully comply with the Authority's BCDR requirements as set out in Schedule 8.6 (Business Continuity and Disaster Recovery) and the Services availability requirements (see Appendix 1 of Annex M to Schedule 2.1 (Non-Functional Requirements & Service Availability)).

Service Catalogue Management

4.9 The Contractor acknowledges and understands that the ITIL process/function of 'Service Catalogue Management' and the Authority requirement of it:

(a) provides a mechanism for the Authority to request Standard Change items as repeatable and pre-defined elements of Operational Change, which are set out in Schedule 2.1, but may be added to by agreement of the Parties;

(b) provides a mechanism for the Authority to request Contract Change items which allow for alterations to Service components that provide the Authority with flexibility and scalability characteristics; and

(c) provides a single source of consistent information on all the current Service Portfolio items as provided by the Contractor, which shall:

(i) ensure that the Authority has an accurate Service Catalogue produced and maintained, for all operational services and those being prepared to be run operationally; and

(ii) ensure that all areas of the Authority can view an accurate, consistent picture of all the Services available and contains both an outwardly Authority-facing view of the Services available and an internal ICT delivery facing view. Such views need to be created that show how the Services are consumed, the business processes they enable, and the levels and quality of service that can be expected.

4.10 The Contractor shall:

(a) maintain the Service Catalogue in accordance with the ITIL process/function of 'Service Portfolio Management', 'Change Management', 'Request Fulfilment' and 'Service Level Management' policies, processes and procedures to ensure that it is always current with the Services;

(b) provide and maintain the Service Catalogue, with updates being agreed with the Authority in advance; and

(c) make the Service Catalogue accessible to the Authority staff, as a simple and intuitive interface and in accordance with Paragraph 2 of this Schedule, assess current maturity levels of existing associated processes and products and provide a detailed assessment and plan for Authority (Hd Mil Pers & Vets Change) approval, for the development and implementation of all Service Catalogue Management processes and associated products.

Service Portfolio Catalogue Items

4.11 The Contractor shall provide Service Portfolio items in the Service Catalogue which shall:

(a) agree and document Service Definitions and all documentation (as detailed in the policies and procedures) for Services listed in the Service Catalogue with the Authority;

(b) provides details of all delivered Services and components, with supporting or referenced information relating to each Service and component, that is consistent and easily understandable for a non-technical audience; and

(c) maintain Service Portfolio items in the Service Catalogue will be delivered as an element of 'Service Portfolio Management'.

Standard Change Catalogue Items

4.12 The Contractor shall provide Standard Change (Operational Change) items in the Service Catalogue which shall:

(a) align to the Change Control Procedure;

(b) have nil cost associated to them;

(c) have an associated standard Impact Assessment which meets the characteristics expected of it in the Change Control Procedure; and

(d) be maintained via the Change Control Procedure as Operational Change.

Contract Change Catalogue Items

4.13 The Contractor shall provide Contract Change items in the Service Catalogue which shall:

(a) have a cost associated to them;

(b) be maintained by the Contractor and agreed with the Authority via the Change Control Procedure as a Contract Change;

(c) ensure the Contract Changes items which can be fulfilled via the Service Catalogue include those that provide the flexibility and scalability to the underlying platforms, including (but not limited to):

(i) the technology scaling elements of the Contractor Solution to meet Authority business demands (including, but not limited to, storage, bandwidth, compute, and memory);

(ii) instantiating new Application Instance for non-Production Environment;

(iii) new interface (for example, simple, medium, complex);

(iv) redirect interface ('Simple', 'Medium', and 'Complex');

(v) decommission interface;

(vi) add or remove a field from an interface ('Simple', 'Medium', and 'Complex'); and

(vii) training.

Service Level Management

4.14 The Contractor acknowledges and understands that the ITIL process of 'Service Level Management' must provide a consistent interface to the Authority for all Service related issues. It must provide the Authority with the agreed Performance Indicators and the required management information to ensure that those targets have been met. Where targets are breached, Service Level Management should provide feedback on the cause of the breach and details of the actions taken to prevent the breach from reoccurring, thus providing a reliable communication channel and trusted relationship with the Authority representatives.

4.15 The Contractor shall:

(a) perform the ITIL process of 'Service Level Management' in accordance with the agreed governance requirements set out in the Schedule 8.1 (Governance);

(b) attend regular 'Service Reviews' and on request with no less than 1 weeks' notice, at an Authority designated site;

(c) ensure new, changed and/or transformed services are provisioned within the requirements of the 'Service Level Management' process of ITSM;

(d) ensure that Service performance measures are included within the design of current and future new or improved Performance Indicators;

(e) ensure all service level agreements are Configurable Items and managed via the Service Asset and Configuration Management Policies, Processes and Procedures;

(f) have processes in place to produce and make available a Service Catalogue for business and technical aspects which contains information including the services provided, the specification, and the availability;

(g) work collaboratively with the Authority to define, document and implement the processes and procedures that will be used to review and revise underpinning contracts and third-party SLAs for the Contractor System;

(h) work with the Authority to define, document and implement the processes and procedures that will be used to agree and record the responsibilities and principles concerning financial charges in relation to the development, implementation, management, operation and maintenance of the Agreement;

(i) ensure that service-level management will liaise with availability management, capacity management, incident management and problem management to ensure that the required levels and quality of service are achieved within the resources agreed with the financial management system;

(j) present to the Authority (Business SMEs and Tech Assurance) the content, structure, reporting frequency and mechanism and presentation format of Performance Indicator information, within the Service Operations Manual;

(k) provide analysis of the performance information to ensure completeness and appropriateness of content for presentation to the Authority (Business SMEs and Tech Assurance) in support of the reporting requirements set out in specific Service Performance Management requirements;

(l) ensure that the Service Operations Manual contains all details of how service performance is captured, measured and reported;

(m) undertake regular formal Service Reviews with the Authority, to assess and review the performance of the Services provided against the Performance Indicators;

(n) provide assurance that system services are being performed in accordance with agreed Performance Indicators and the Service Operation Manual, allowing the Authority to perform checks upon any aspect of the ICT systems that comprise the Services;

(o) ensure the ITIL processes of 'Service Level Management' are in place to provide continual identification, monitoring and review of the expected Performance Indicators to the IT services specified in this Agreement;

(p) provide monitoring, reporting and assurance of service level compliance through monitoring performance and providing performance reporting in accordance with the SLAs in this Agreement; and

(q) periodically carry out the preparation and review of Service Performance Reporting with The Authority.

Security Management

4.16 The Contractor acknowledges and understands that the ITIL process of 'Security Management' is necessary to ensure the confidentiality, integrity and accessibility of the IT Services, their data and infrastructure and, in the context of this Agreement and the Services to be provided, this is necessarily a core area that has specific obligations that are set out in Schedule 2.4 (Security Management), which the Contractor must adhere to. The obligations as set out in this section are necessary to ensure that 'Security Management' is undertaken in the context of ITSM, with the interactions and inter-dependencies to other processes and functions that it is required to operate within.

4.17 The Contractor shall provide the ITIL 'Security Management' processes and functions in accordance with Schedule 2.4 (Security Management);

Supplier Management

4.18 The Contractor acknowledges and understands that ITIL 'Supplier Management' process defines the responsibilities of the Contractor, in support of the Authority, in the monitoring and reviewing the performance and engagement of all Suppliers in complying with obligations to the Policies and Procedures set down by the Contractor and their contracted obligations agreed with the Authority. This is a valuable process to the Authority as it ensures that the day-to-day engagement with other Suppliers is managed to ensure that all Suppliers operate to a common understanding and performance level. The main objectives for the Supplier Management process are:

(a) work with third party Suppliers to ensure conformance and adherence to agreed policies and procedures;

(b) manage the take on of new third party suppliers;

(c) manage the non-compliance to policies and procedures by any third party supplier;

(d) manage the day-to-day operational relationship with Related Third Party;

(e) conduct regular performance reviews with Other Suppliers; and

(f) provide an interface for formal communications from all Suppliers third party suppliers and the Authority.

4.19 The Contractor shall:

(a) manage the performance of the third party suppliers and the Authority against the agreed Third Party Contract;

(b) monitor and report quarterly to the Authority on the behaviours of the third party suppliers and the Authority in engaging with and applying the terms of the Agreement;

(c) identify process improvements and recommendations for consideration as part of the performance review;

(d) in accordance with the 'Supplier Management' policies and procedures arrange, coordinate and manage regular performance reviews with the third party suppliers regarding their respective Services and agreed process improvement plans;

(e) support the third party suppliers and the Authority to identify process improvements and recommendations for consideration as part of the performance review;

(f) convene and manage a quarterly Service Review Board with the third party suppliers, at which the Authority may also attend;

(g) provide regular Management Information in support to the Service Review Board, including (but not limited to) appropriate commercial and strategic management functions;

(h) provide a secretariat function to the Service Review boards and must:

(i) ensure that all agreed improvement actions during the course of the Service Review board are captured;

(ii) manage all agreed improvement actions to completion as part of the ITIL process of 'Continual Service Improvement';

(iii) manage agreed actions that require activities involving more than 1 other third party supplier; and

(iv) produce (in consultation with the Authority) a monthly third party supplier 'Scorecard' showing the comparable performance of All Suppliers against an agreed set of appropriate measures;

(i) identify and maintain a complete documented view of the supply chain across the Service provision and across the end-to-end Service provision;

(j) identify and manage the risks across the Service supply chain in accordance with the Risk Management Policies and Procedures; and

(k) ensure all risk information from Suppliers is made available to the Authority's Risk Register in accordance with Schedule 8.1 (Governance).

5 SERVICE CHANGE

5.1 The Contractor shall provide the ITIL processes and functions of 'Service Change' in accordance with the Change Control Procedure. For the avoidance of doubt, 'Service Change' refers to the ITIL stage of 'Service Transition'.

5.2 **Change Delivery Strategy**

(a) 30 days prior to the Operational Services Commencement Date, the Contractor shall prepare and submit to the Authority a draft Change Delivery Strategy.

(b) upon receipt of the draft Change Delivery Strategy:

(i) the Authority shall approve the draft Change Delivery Strategy; or

(ii) if the Authority has proposed changes to the draft Change Delivery Strategy, the Parties shall meet and agree the proposed changes (such agreement not to be unreasonably withheld or delayed) by no later than 15 days prior to the Operational Services Commencement Date.

(c) Once the draft Change Delivery Strategy is agreed between the Parties, the Contractor shall implement, deliver, maintain and adhere to the Change Delivery Strategy from the Operational Services Commencement Date.

5.3 **Forward Schedule of Change**

(a) 30 days prior to Operational Services Commencement Date and each 24 months thereafter, the Parties shall develop and agree a Forward Schedule of Change to detailing all Changes envisioned to be included in subsequent 24 month period.

(b) The Contractor shall provide access to the Forward Schedule of Change to the nominated Authority staff via and the Authority Systems.

(c) The Forward Schedule of Change shall specify:

(i) the number and timing of Releases for Changes; and

(ii) details of all Change approved at the JCAB which are yet to be implemented;

(iii) details of future Changes identified by the Contractor (and agreed for inclusion in the Forward Schedule of Change with the Authority);

(iv) details of the level of Contractor resource required for the implementation and delivery of the Changes;

(v) key timelines and key delivery points; and

(vi) any other information that the Authority may reasonable require from time to time in order to ensure that the Forward Schedule of Change shows all

Changes which are being implemented and delivered at any time, and for each month the Changes which are being implemented and delivered.

(d) The Joint Change Advisory Board shall review and approve the Forward Schedule of Change on a weekly basis (or any other time period as agreed between the Parties).

(e) The Contractor shall be responsible for implementing all Change included in the Forward Schedule of Change. The Authority shall be entitled to amend the Forward Schedule of Change or the order of priority set out therein in accordance with this Paragraph 5.3.

(f) The Contractor shall inform the Authority of any potential deleterious effects of a Change and any adverse effects of the Change in terms of delivery of the Services and/or the Authority's business before implementation of the Change, identifying and recommending risk mitigation or remedial actions to minimise or remove such deleterious or adverse effects.

(g) If you Parties agree a change to the Forward Schedule of Change, the Contractor shall perform an impact analysis for such change within 2 Working Days of it being agreed by the Parties and submit the impact analysis to the Authority for review and approval of the change at the next available JCAB.

(h) The Contractor shall notify the Authority's Change Manager of any issues or risks which may delay the delivery of any Change and/or Release detailed in the Forward Schedule of Change within 1 Working Day of the issue or risk being raised providing mitigations where appropriate.

(i) The Contractor shall stop the delivery of any planned Change that would compromise the continuation of Services, unless expressly overridden by the Authority.

(j) On request by the Authority, the Contractor shall:

(i) terminate a Change before implementation;

(ii) terminate a Change during implementation; and

(iii) within the time period specified by the Authority at the time of such request, back out of an implemented Change, reverting to the configuration of the live, development or test environment (as appropriate) prior to such implemented change.

5.4 **Change Management**

(a) The purpose of Change Management is to identify, control and account for Service Assets and Configuration Items, protecting and ensuring their integrity during the Term.

(b) The Contractor shall implement, deliver, maintain and adhere to the Change Management component of ITSM, across all elements of the Services, to support delivery of, while wholly adhering to, the Schedule 2.1 (Service Description) and Schedule 8.2 (Change Control Procedure), which shall:

(i) respond to Changes in accordance with the priorities of the Authority;

(ii) contribute to improved estimations of quality, time and cost of change;

(iii) implement Changes to meet the Authority's requirements, while seeking to optimise efficiency;

(iv) contribute to meeting operational governance, legal, contractual and regulatory requirements;

(v) reduce the number of Changes that fail to deliver the requirements of the Change and reduce the amount of service disruptions, defects, and re-works;

(vi) deliver Change consistently and promptly within the expected timescales for Change;

(vii) aid in productivity of resources by minimising disruption due to high levels of unplanned or emergency change thus improving the efficiency;

(viii) provide a single tracking facility for all Changes through the Change progress and to Service Assets;

(ix) assess the risks associated to the Changes to the Services, both new and existing; and

(x) increase service quality through appropriate impact assessment of Changes, thus preventing Incidents.

5.5 **Change Management System**

(a) Within 3 months of the Operational Services Commencement Date, the Contractor shall provide, maintain and support the Change Management System.

(b) From the Operational Services Commencement Date to the provision of the Change Management System, the Contractor shall establish and agree a manual system for the logging and monitoring of all Change Requests.

(c) The Change Management System shall:

(i) enable a Change Request to be raised electronically by either Party;

(ii) allocate a unique reference number to each Change Request;

(iii) record all costs and charges expended through the delivery of Change, including planned expenditure over a rolling 6 month period;

(iv) provide a reporting instance to enable Management Information to be retrieved;

(v) record any agreed key milestones and deliverables;

(vi) enable restricted visibility to Authority sensitive data; and

(vii) be delivered in accordance with all NFRs detailed in in Appendix 1 (Non-Functional Requirements & Service Availability) of Annex M (Technical & Applications) to Schedule 2.1 (Services Description).

(d) For any Service Downtime of the Change Management System, the Authority Change Manager shall be given 5 Working Days prior notice of such Service Downtime, unless otherwise agreed by the Authority.

(e) For any Service Outage of the Change Management System during Core Hours, the Contractor shall rectify such Service Outage in accordance with the Incident Resolution Matrix (as detailed in Appendix 2 (Incident Resolution Matrix) of Annex M (Technical Applications) to Schedule 2.1 (Services Description)).

5.6 **Project Management**

(a) The Contractor shall implement, deliver, maintain and adhere to the project management component of ITSM, across all elements of the Service ensuring the service for the introduction of new or changed services has the following activities embedded across the Project Management lifecycle:

(i) develop a strategy for transition;

(ii) ensure proven and transparent project delivery methodologies (Agile, waterfall, hybrid) are established and appropriately governed;

(iii) prepare for and plan for transition;

(iv) identify, manage and limit the risks to service interruption;

(v) complete Service Requirements capture;

(vi) complete Service Design;

(vii) confirm Service Design with the approval body;

(viii) complete Testing;

(ix) confirm Service Release and Deployment readiness; and

(x) perform Service handover and review (as defined in ITIL).

(b) The Contractor shall ensure the that Project Management component of the ITSM framework is applied across all elements of the MilPers and Vets service provisions as agreed with the Authority.

5.7 **Service Design Documentation**

(a) No later than 5 Working Days prior to any Critical Design Review, the Contractor shall provide the Service Design Documentation to the Authority (Change Manager). Such Service Design Documentation should be provided to a level of detail, accuracy and completeness that is defined by a Contractor's proposed documentation methodology as set out in the Change Delivery Strategy in alignment with the Joint Architecture Governance Framework and shall include, but not be limited to:

(i) 'Outline Solution Document';

(ii) 'Detailed Solution Design';

(iii) 'Data Integration, Acquisition, Conversion and DQ Strategy' (as defined in Annex H (MiI MIT & Data));

(iv) 'Data Structures and Models' (as defined in Annex H (MiI MIT & Data));

(v) 'Functional Specification';

(vi) ‘Requirements Traceability Matrix’;

(vii) 'Component Technical Design';

(viii) 'Business Process Model';

(ix) 'Logical Technology Model';

(x) 'Physical Technology Model';

(xi) 'Logical Application Model'; and

(xii) 'Physical Application Model".

(b) All Service Design Documentation created or updated as a result of a Change shall be shared by the Contractor with the Authority (Technical Assurance) when completed or shared on request of the Authority (Technical Assurance), in a draft or interim state.

(c) The Contractor shall retain and make available to the Authority on written request all information, whether written, electronic or otherwise, concerning all Change Requests, including receipts of payments (where relevant), work undertaken, time

involved for its respective employees and any third Parties for a period of 2 years from the later of:

(i) the date of expiry or termination of this Agreement;

(ii) the date on which the Contractor and any relevant sub-contractors complete all required Exit Services to the reasonable satisfaction of the Authority; or

(iii) the date of termination or expiry of the relevant Contract Change Agreement and/or Contract Change Note (as applicable).

5.8 **Release and Deployment Management**

(a) The Contractor shall implement, deliver, maintain and adhere to the Release and Deployment Management component of ITSM which shall interface with the ITIL process of Change Management to ensure protection of the IT Environments using formal procedures and checks and minimising downtime caused by the implementation of Releases across the Contractor Systems.

(b) The Contractor shall undertake all Release and Deployment Management activities in accordance with agreed policies and procedures for Release contained in the SOM which shall comprise the following stages:

(i) build, test and deployment preparations for the Release;

(ii) coordinate, manage, and provide support to the Authority for all Testing phases of the Release in accordance with Schedule 6.2 (Testing Procedures);

(iii) plan and prepare for deployment of the Release;

(iv) transfer and deploy the Release and retire previous service elements and decommission any redundant ICT;

(v) provide 'early life support', being early stage support following the Release;

(vi) verify service deployment; and

(vii) review and close deployment.

(c) The Contractor shall ensure that the Release and Deployment Management adheres to the following principles:

(i) planning the rollout of Software;

(ii) ensuring the totality of the Contractor Systems Environment landscape and Application Instances are maintained in a coherent manner;

(iii) designing and implementing procedures for the distribution and installation of changes to IT systems in the most efficient and least disruptive manner;

(iv) effectively communicating and managing expectations of the Authority during the planning and rollout of new releases;

(v) controlling the distribution and installation of changes to IT systems;

(vi) controls must be in place to ensure the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure; and

(vii) ensure that quality control during the development and implementation of new hardware and Software, ensuring that all software meets the demands of the business processes.

5.9 **Release categories**

(a) Release categories shall include but not be limited to:

(i) Major Releases of Software and/or Hardware, normally containing large amounts of new functionality or capability across multiple Service applications, in addition to fixes and patches to correct Problems;

(ii) Minor Releases of Software and/or Hardware, normally containing a small self-contained set of functional enhancements to individual Service applications, or fixes and patches to correct Problems;

(iii) Emergency Releases of Software and/or Hardware fixes and patches, normally containing the corrections to a small number of known problems, determined to be such according to an urgency in applying the Change, which may be a result of Incident resolution;

(iv) Out of Release, where Change is delivered in isolation of other changes, updates, or fixes and which is usually limited in scope, of a low risk, and of a common disposition (for example, a Standard Change).

(b) The Contractor shall provide the capability to roll back Releases if they are unsuccessful. This must be Tested and evidence of Acceptance is to be provided to the Authority.

(c) Unless otherwise agreed with the Authority, the Contractor shall prepare and maintain a Release Plan for all Major and Minor Releases and make such Release Plan available to the Authority on request within the following timescales:

(i) no later than 20 Working Days prior to a minor Release; and

(ii) no later than 2 Months prior to a Major Release

(d) Each Release Plan shall be reviewed weekly as part of the JCAB with any updates and/or amendments being applied within 2 Working Days of agreement of such Release.

(e) Release Plans are to record as a minimum the following:

(i) all Changes scheduled for delivery within a Release, including all Emergency Change and/or all changes to support system integrity including, but not limited to, fixes, patches;

(ii) Key Milestones;

(iii) risk assessment of deployment;

(iv) Service impacting events in the schedule, with outages established and defined;

(v) resource profile (RACI) for Contractor and Employee engaged in activity;

(vi) the schedule of Release across the entirety of the Contract Systems Environment landscape;

(vii) all test phases to be conducted, including start and finish dates of each phase; and

(viii) Deliverables and target dates.

(f) The Contractor shall provide adequate and appropriate support resources for a period of time as agreed with the Authority, or defined by the Release Plan, after each Release deployment to monitor, collect performance data relating to the new Release, resolve operational issues, including any teething troubles with the new Release and to confirm Release stability.

(g) The Contractor shall define and agree the handover to support process for any new/changed Services.

5.10 **Critical Design Review**

(a) The Contractor shall:

(i) provide the Authority's Change Manager with all documentation required for a Critical Design Review no later than 2 Working Days prior to the relevant Critical Design Review;

(ii) deliver and facilitate a Critical Design Review for each Minor and Major Release on completion of each Release design or in any case no less than 60 Calendar Days prior to Release dates for each Major Release or as agreed with the Authority (Change Mgr) for all Minor Releases, which shall be

attended by the Contractor and Authority as agreed by both Parties, unless otherwise agreed with the Authority; and

(iii) provide the records of discussion to the Authority's Change Manager within 2 Working Days of the relevant Critical Design Review taking place.

(b) Critical Design Reviews shall include, but not be limited to, the following:

(i) the deployment schedule, including the timing and duration of the Release;

(ii) the expected downtime and/or period of limited service of the Services during the Release;

(iii) the implementation process;

(iv) the effect on any interfaces during Release implementation;

(v) the impact of the Release;

(vi) the risks associated with the Release and all mitigations;

(vii) the processes for restoring the solutions to live running if an operational emergency occurs during the upgrade process;

(viii) the process for rolling back the solutions should the upgrade not be successful;

(ix) the support required from Users during the Release process; and

(x) the knowledge transfer requirements of the Release to the Authority.

(c) The Contractor shall record and distribute to all attendees the minutes following each Critical Design Review.

5.11 **Operational Readiness Review**

(a) The Contractor shall:

(i) provide the Authority's Change Manager with all documentation required for an Operational Readiness Review no later than 2 Working Days prior to the relevant Operational Readiness Review;

(ii) deliver and facilitate an Operational Readiness Review for any Change resulting in a change to the IT environment delivered as part of Transformation (or as directed by the Authority), no later than 3 Working Days prior to the deployment of each Release. which shall be attended by the Contractor and Authority as agreed by both Parties, unless agreed with the Authority; and

(iii) provide the records of discussion to the Authority's Change Manager within 2 Working Days of the relevant Operational Readiness Review taking place.

(b) Operational Readiness Reviews shall include, but not be limited to, the following:

(i) a list of all Changes to be deployed;

(ii) Release Plan review;

(iii) review of any Critical Design Review actions;

(iv) the impact of the change(s) on existing services and/or processes;

(v) the impact on ICT;

(vi) testing validation results;

(vii) back out plans; and

(viii) BCDR.

(c) The Contractor shall record and distribute to all attendees the minutes following each Operational Readiness Review.

5.12 **Testing**

All Change shall be subject to Testing conducted in accordance with the minimum requirements specified in Schedule 6.2 (Testing Procedures).

5.13 **Service Asset and Configuration Management**

In addition to the Contractor's obligations in respect of Technical Refresh, this paragraph sets out additional Contractor obligations with regard to the provision, support and maintenance of the Software and Hardware used to support and deliver the Services.

5.14 **Decommissioning of Software or Hardware**

(a) **Removal or replacement**

Should any Software or Hardware be removed, withdrawn or replaced, such removal, withdrawal or replacement shall be assessed by the Contractor to understand its impact on the Charges. In the event that Software or Hardware is removed, replaced or is not upgraded, the Contractor must provide the detail to substantiate the resultant reduction in Charges. Upon the agreement of the appropriate reduction to the Charges, (the Parties acting reasonably), the Charges shall be reduced by the agreed amount.

(b) **Decommissioning**

The Contractor shall ensure that the decommissioning of any equipment, hardware, software and facility/building is to be undertaken in accordance with MOD policy or guidelines and the Authority will be kept informed at all stages, from intent to disposal:

(i) the Authority to be informed in writing by the Contractor, immediately when the intention is known, to decommission any part of the IT estate including buildings and facilities, regardless of the method of disposal;

(ii) decommissioned state of the facility or equipment is to meet the standards and requirements agreed with the Authority in writing before commencement; and

(iii) during decommissioning, the authority is to be given option for high value and specialist equipment to be retained for future use.

5.15 **Retained Software Agreements**

(a) Without prejudice to Paragraph 5.15(f) and subject to the Contractor obtaining the rights referred to in Paragraph 5.15(d) below, the Authority hereby appoints the Contractor to manage and administer the Retained Software Agreements on behalf of and solely for the benefit of the Authority and as otherwise required under this Agreement, such obligations to include:

(i) complying with the obligations imposed on the Authority under each of the Retained Software Agreements;

(ii) ensuring that the Authority is appropriately licensed to use the Software in order to receive the Services in accordance with the provisions of this Agreement;

(iii) not doing or allowing anything to be done which would cause the Authority to be in breach of any Retained Software Agreement;

(iv) at its own cost, paying all charges under each of the Retained Software Agreements as they arise or fall due for payment; and

(v) giving the Authority at least 30 days' notice of any Key Decision Date in respect of each of the Retained Software Agreements.

(b) The Contractor shall not, without the prior written consent of the Authority (such consent not to be unreasonably withheld or delayed):

(i) renew, modify, extend, terminate or cancel any Retained Software Agreement;

(ii) request or grant any consents or waivers under any Retained Software Agreement; or

(iii) take any legal action (or any precursor to such action) in the name of the Authority or otherwise in respect of any Retained Software Agreement.

(c) The Contractor, with effect from the Operational Service Commencement Date, shall be responsible for compliance with the terms of the Retained Software Agreement (save to the extent specified in Paragraph 5.15(f)) and shall be responsible for and shall not raise any claim, demand or proceeding against the Authority in respect of any breaches or defaults under those contracts unless such breaches or defaults are due to any failure by the Authority to comply with any provisions preventing or restricting the management of the Retained Software Agreement by any third party or relate to any claim made against the Contractor by a Third Party Contractor relating to a breach by the Authority prior to the Operational Service Commencement Date of the Retained Software Agreement.

(d) To the extent required for the purposes of performing the Services under this Agreement, the Authority shall use its reasonable endeavours to obtain from each relevant Third Party Contractor, rights to use the software and all Intellectual Property which has been licensed to the Authority in the Retained Software Agreements, to be effective on the Service Commencement Date. The Contractor shall provide such assistance as may be reasonably required by the Contractor in support of its obligations.

(e) In relation to any Retained Software Agreements in respect of which rights to use have not been obtained prior to the Operational Service Commencement Date, the Parties shall, in respect of the period from the Operational Service Commencement Date until the date of any subsequent grant of the relevant rights, discuss and agree options for alternative arrangements (indicating the arrangements preferred by the Contractor) in respect of such licences which will ensure that the Authority is not unduly prejudiced or adversely affected by the failure to obtain such rights and implement such arrangements as are agreed by the Authority and the Authority shall bear the costs and expenses associated with seeking such rights and making any such alternative arrangements.

(f) For the avoidance of doubt the Authority shall retain responsibility for enforcing its rights and remedies under the Retained Software Agreements. The Contractor shall, at no additional cost, provide such assistance and information as is reasonably required by the Authority to enable the Authority to enforce such rights and remedies.

5.16 **Software Services**

(a) The Contractor shall be liable for the Charges as set out in Schedule 7.1 (Charges and Invoicing) and will include all costs and charges:

(i) levied by the relevant Software licensor/vendor/reseller in respect of a Software application (including any Replacement Software Application) including, without limitation, all costs and charges relating to:

(ii) the licensing (including all and any Software licensor/vendor/reseller upgrades; updates; patches; workarounds; versions and releases including new functions available in the upgraded or updated Software application);

(iii) the upgrades and transformations that are required to achieve the agreed Contractor proposal, in relation to Transformation and Technical Refresh;

(iv) payable for support and maintenance;

(v) any change in Software licensor/vendor/reseller pricing models;

(vi) payable for Software compatibility;

(vii) payable for Software extended support;

(viii) payable for any re-platforming or repackaging of the software applications;

(ix) payable for all alterations and remediation resulting from an upgrade, update, version or release change to the Software;

(x) payable for alterations and remediation resulting from a modification or patch change to the Software;

(xi) payable for all necessary configuration, integration, testing and implementation;

(xii) payable for Contractor Personnel error or omission; and

(xiii) payable in respect of the configuration, installation, testing and implementation of the Software application (including any Replacement Software Application),

together the ("**Software Services**").

(b) The Charges relating to the Software Services are in respect of all Software required to provide the Services in accordance with the provisions of this Agreement including the:

(i) Contractor Software;

(ii) Contractor Third Party Software;

(iii) Authority Software; and

(iv) Authority Third Party Software.

5.17 **Ongoing review**

Without prejudice to the Contractor's obligations during the Term in respect of Continuous Improvement, the Contractor shall proactively monitor its and the Authority's use of the Software in order to ascertain ways in which the Contractor can reduce the Authority's costs in respect of the Software. Such activities may include: the consolidation; rationalisation; replacement or removal of items of Software; identifying where the Authority is 'over-licensed' in respect of an item of Software; advising the Authority as to whether or not the Authority should implement any Upgrade issued by the Software licensor/vendor/reseller.

5.18 **Withdrawn Software Applications**

(a) The Contractor shall continuously and actively review all software and vendor bulletins, briefings, industry communications, and any applicable communication means the vendors provide for product roadmap and strategic planning for their products, in order to advise the Authority and meet its obligations within this Agreement.

(b) The Contractor shall, within 10 Working Days of it coming to its attention that the support and maintenance of a Software application is to be withdrawn by the Software licensor/vendor/reseller ("Withdrawn Software Application"), in alignment with:

(i) provide a list of alternative software applications that the Contractor considers suitable as a replacement for the Withdrawn Software Application ("**Alternative Software Application**");

(ii) provide an assessment setting out (i) the differences between the features and functionality of the Withdrawn Software Application and each of the Alternative Software Applications and (ii) the impact, if any, on the Technology Roadmap the Authority's then current ICT policy; and

(iii) provide details of the Alternative Software Application that the Contractor recommends together with its reasons for recommending such application; and

(iv) follow the Change Management Procedure to progress replacement, when agreed with the Authority (Tech Assurance).

(c) The Parties shall meet to discuss and agree which Alternative Software Application shall replace the Withdrawn Software Application ("**Replacement Software Application**").

(d) The Replacement Software Application shall be introduced into the Services (and shall be subject to the provisions of this Agreement) by way of an Operational Change.

5.19 **Software Management**

(a) The Software is to be managed at all times by the Contractor in full alignment with the Service Asset and Configuration Management Procedures as detailed in Schedule

8.2 (Change Control), implementing and Configuration Management Database (CMDB).

(b) The CMDB shall record, as a minimum, the following information about the Software (as amended from time to time with the agreement of the Parties, not to be unreasonably withheld or delayed):

- Software Asset ID
- Name
- Supplier
- Original Cost – if know by the Contractor
- Date of Purchase
- Purchase Order Number
- Invoice Number
- Version number
- Location of master copy of software
- Details of any 'patches' loaded
- Configuration information
- Licence information – for example:
  - Licence Number
  - Number of users/licences
  - Type / term of licence etc
- Details of support contract
- Current number of users
- Requests for Change (RFC) affecting this asset
- Incidents/Problems affecting this asset
- Details of where the licences are used:
  - Hardware Asset ID number
  - Specific Server
  - Named person
  - Named location and/or Cost Centre
- Date asset added to database
- Date asset verified or audited in database
- Date asset removed from database
- Asset removal authorised by

(c) The Contractor will provide and maintain the Software Library (as a related component of the CMDB) that will securely store, control and organise all Software including management of:

(i) the master copy of the Software;

(ii) backup copies of the Software for Disaster Recovery etc.;

(iii) distribution copies on free-standing media or servers;

(iv) Software licence certificates or other proof of licence;

(v) Software licence keys or 'pass codes';

(vi) the terms and conditions of the licence;

(vii) any software maintenance authorisation codes, if applicable;

(viii) master copies of software documentation, manuals, etc.; and

(ix) any information relating to software upgrades and patches

(d) The Contractor shall record the following details (relating to the Software) within the CMDB:

(i) an up to date and accurate record of the Software licences and maintenance agreements relating to each Software application;

(ii) automated processes connected to managing Software licences and compliance;

(iii) cross reference Software licence entitlement with consumption – whatever the unit of measure (hardware, User or whether or not concurrent);

(iv) Associate Software licenses with related contract information;

(v) measure consumption against licence commitment (licence metering);

(vi) ensure that when a copy of the Software is installed, the appropriate number of licences are allocated so as to ensure that the Authority is not in breach of any licence requirements;

(vii) drive streamlined purchasing based on agreed contracts;

(viii) master copies of all installation/configuration Software for the operating system and associated drivers;

(ix) proof of any applicable OEM licensing in relation to the Software pre-installed on the hardware; and

(x) integrated fully with existing systems including inventory, procurement and the CMDB.

(e) The Contractor is responsible for ensuring that the terms and conditions governing the use of all Software are adhered to and shall report any actual or attempted breaches of such terms immediately to Authority's Security Officer.

(f) The Contractor shall maintain and (when requested to by authorised staff in the Authority) provide ‘proof of licenses’ in original installations, any subsequent upgrades and OEM arrangements.

(g) The Contractor shall (at least every six months) perform regular reconciliation of all Software used in the delivery of the Services in order to ascertain what Software is being used in relation to the licenses purchased and promptly bring any discrepancies to the Authority’s attention with a plan for its resolution (by way of a report).

(h) The Contractor shall advise on and work with the Authority to ensure the most beneficial and ‘value for money’ software licensing arrangements.

(i) The Contractor shall comply with the Authority's guidelines and principles in this area from the Federation against Software Theft (FAST), the Business Software Alliance (BSA) and the Control Objectives for Information Technology (COBIT) framework developed by the IT Governance Institute.

5.20 **Software Licence Management and Compliance**

(a) The Software is to be managed at all times by the Contractor In full alignment with the Service Asset and Configuration Management Procedures as detailed in Schedule 8.2, implementing a Configuration Management Database (CMDB).

(b) The elements set out in this section refer to the obligations of the Contractor to manage on behalf of the Authority, and the adherence to Software licensing terms and conditions for the services (Applications and COTS Software) consumed by the Authority as recorded by Schedule 5 of the Agreement.

(c) The Contractor shall manage compliance with all Software licences by monitoring and auditing all Software use on behalf of the Authority and in accordance with the Authority’s Software Management Policy.

(d) The Contractor shall ensure that all necessary support is provided to any Auditor or any external licence audits requested by the Authority and/or authorised Third Parties.

(e) The Contractor shall provide appropriate auditing tools including software licensing in support of Licence Management.

(f) The Contractor shall monitor and report on license usage comprehensively and accurately at all times.

(g) The Contractor shall proactively monitor the use of all Software in order to maintain strict compliance, including but not limited to:

(i) Immediately notifying and advising the Authority of any Software license compliance issues identified within the Authority's ICT environment or associated with the use of Services provided to the Authority;

(ii) Software associated with Services, ensure appropriate provisioning and availability of Software;

(iii) Ensure appropriate monitoring is put in place for the purposes of identifying the presence of any unauthorised or non-standard Software; and

(iv) Providing periodic reporting of license information and compliance to Authority, as required.

(h) The Contractor shall manage the procurement of all Software licences provided to the Authority on behalf of the Authority, and utilise the licences in the most cost-effective manner available.

5.21 **Hardware**

(a) The Contractor shall ensure that the hardware is:

(i) housed, used and maintained in accordance with the provisions of this Agreement and the manufacturer's recommended instructions;

(ii) subject to an appropriate support and maintenance agreement for the duration of the Term in order to enable the Contractor to continue to achieve the Performance Indicators and must have a minimum of two (2) years support (of a standard not less than that provided during the Term) post expiry or termination of this Agreement; and

(iii) not used to provide services to any third party (without the prior written consent of the Authority);

(b) In the event the Contractor fails to refresh all or part of the Hardware in accordance with the provisions of this Schedule or within a reasonable time thereafter as agreed with the Authority, the Contractor shall, on request by the Authority, reimburse the Authority (on a pound for pound basis) for that part of the Hardware that has not been refreshed.

5.22 **Hardware Management**

(a) The Hardware is to be managed at all times by the Contractor In full alignment with the Service Asset and Configuration Management Procedures as detailed in Schedule 8.2, implementing a Configuration Management Database (CMDB).

(b) The CMDB shall record, as a minimum, the following information about the hardware (as amended from time to time with the agreement of the Parties, not to be unreasonably withheld or delayed):

- Hardware Asset ID
- Make
- Model
- Hardware configuration (memory, processor, disk, etc)
- Serial Number(s)
- User(s)
- Location and ‘Owner’
- Department
- Date of Purchase
- Purchase Price / Replacement Cost
- Supplier
- Warranty details
- Purchase Order Number
- Invoice Number
- Lease information, if applicable
- Software Installed (Name, version numbers, etc)
- Attached peripherals (Monitor, Printer, Scanner, PDA etc)
- Relevant Configuration Information
- Access rights
- Requests for Change (RFC) affecting this asset
- Incidents/Problems affecting this asset
- Date asset added to database
- Date asset verified or audited in database
- Date asset removed from database
- Asset removal authorised by

(c) The Contractor will securely store, control and organise the following documentation and materials within the hardware library including management of:

(i) All documentation relating to the hardware; and

(ii) Warranty information including suitable proof of purchase for the supplier to honour the warranty.

5.23 **Knowledge Management**

(a) General Principles

(i) The Contractor shall implement, deliver, maintain and adhere to the Knowledge Management component of ITSM, across all elements of the Services and ensure that Knowledge Management at all times effectively interfaces with all appropriate ITIL processes.

(ii) Knowledge Management must be the primary method that allows individuals and teams to share data, information and knowledge about all facets of service. Knowledge Management is to include, but is not limited to:

(A) User profiling and demand characteristics;

(B) Service Desk scripting and Service Knowledge Management System; and

(C) Known Errors signed off before deployment.

(b) Service Knowledge Management System

(i) To support effective Knowledge Management the Contractor is to design, implement and maintain Service Knowledge Management Systems (SKMS) and tools for collecting, storing, managing, updating, analysing and presenting all the knowledge, information and data to manage the full lifecycle of IT services.

(ii) In developing the SKMS, the Contractor shall:

(A) Establish data and information requirements;

(B) Define the information schema; and

(C) Establish data and Information Management Procedures.

(iii) The SKMS shall contain data and information, including but not limited to:

(A) Methods to resolve incidents;

(B) Known errors;

(C) Service desk scripts;

(D) Self-help articles; and

(E) Frequently asked questions.

(iv) The Contractor is to ensure the Authority can access the SKMS via MOD platforms and Operating Systems.

(v) The Contractor shall cooperate with the Authority to perform conformance reviews and audits from time to time, as agreed with the Authority, to ensure the integrity and accuracy of data in the SKMS. Where data is found to be inaccurate or, incomplete, the Contractor shall correct or remove the data as agreed with the Authority.

5.24 **Change Closure and Review**

(a) The Contractor shall ensure Changes are closed within the agreed timelines as set out in the Service Operations Manual when authority has been received by the Authority.

(b) The Contractor shall report the non-implementation and/or delivery of an approved Change to the Authority Change Manager as soon as possible and in any event within 20 Working Days of the date at which the Change should have been delivered, detailing the following:

(i) a description of aspects of the approved Change that have not been implemented and/or delivered;

(ii) an explanation of the cause of the non-implementation and/or delivery;

(iii) a summary of the consequences on the delivery of the Services affected by the non-implementation and/or delivery;

(iv) a plan setting out the proposal showing how and when the approved Change will be implemented and/or delivered;

(v) whether the failure to implement and/or deliver is attributable to the Contractor or the Authority and, if caused by both Parties, which proportion it believes is attributable to each Party. Thereafter, the Contractor shall continue to update the Authority as agreed on what remedial steps it is taking to remedy the failure until such time as the relevant approved Change has been implemented and/or delivered. For the avoidance of doubt, all rectification costs are at the Contractor's risk to the extent that the failure is not caused by the Authority; and

(vi) where the failure is attributable to the Authority, the Contractor shall, upon request, produce and provide to the Authority Change Manager an estimate of the costs (for consideration by the Authority) that it considers the Authority will have to bear for the rectification of the failure.

(c) The Contractor shall:

(i) conduct a Post Implementation Review to include lessons learned:

(A) for all Releases (except for Major Change), within 20 Working Days of the delivery of the Release; or

(B) for Releases for Major Change, within 20 Working Days of the delivery of the Change; and

(ii) within 10 Working Days of such review being conducted, provide the Authority (Change Manager) with a copy of the Post Implementation Review findings.

(d) The Contractor shall initiate and maintain a process to capture and present to the Authority, as and when requested by the Authority, User feedback relating to Changes deployed.

6 SERVICE OPERATION

Service Operation stage

6.1 The Contractor acknowledges and understands that the purpose of the ITIL process of 'Service Operation' stage is the coordination and delivery of the activities, processes and functions required to deliver and manage the Services to agreed levels, to the Authority. Service Operation covers the responsibilities for the ongoing management of the technology used to deliver and support all Services.

6.2 The Contractor shall:

(a) implement, deliver, maintain and adhere to the 'Service Operation' process area of ITSM, across all elements of the Service;

(b) put in place 'Service Operation' processes and measures to achieve best practice for achieving the delivery of agreed Performance Indicators; and

(c) put in place 'Service Operation' functions include technical management, application management, operations management and service desk as well as, responsibilities for staff engaging in 'Service Operation'.

Application Management

6.3 The Contractor shall ensure the required set of best practices, processes, and measures are in place to ensure the required level of quality for software development and support through

the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

IT Operations Management

6.4 The Contractor shall:

(a) ensure the required set of best practices, processes and measures are in place to ensure the required level of quality for software development and support through the life-cycle of software development projects, with attention to gathering and defining requirements that meet business objectives;

(b) from Operational Service Commencement Date, create, maintain and make available for the Authority's approval on a weekly basis, an 'Operational Schedule Plan' which shall include:

(i) data consisting of (but not be limited to) all scheduled jobs, core business process activities, interfaces, Service Change and scheduled maintenance activity on the complete Service and their components;

(ii) to make available scheduled activity data at hourly, daily, weekly and monthly levels of detail;

(iii) covering the upcoming 12 month period and all previous data;

(iv) on an hourly and daily level for next 4 week period, while future periods can be summarised to daily level and aggregated to weekly and monthly summarisations as necessary;

(v) which is made available as a real-time calendar centric graphical format on a suitable web-based portal; and

(vi) an accurate representation of the planned operational activities; and

(c) ensure that the ITIL function of 'IT Operations Management' provides robust documented processes and procedures and should be concerned with specific sub-processes, including (but not limited to):

(i) output management;

(ii) job scheduling;

(iii) backup and restore;

(iv) network monitoring and management;

(v) system monitoring and management;

(vi) database monitoring and management; and

(vii) storage monitoring and management.

Identity and Access Management

6.5 The Contractor acknowledges and understands that the ITIL process of 'Identity and Access Management' is the process of granting authorised End Users the right to use a Service and helps to protect the confidentiality, integrity and availability of assets and information.

Event Management

6.6 The Contractor acknowledges and understands that the ITIL process and measures of 'Event Management' must be in place to indicate when something is not functioning correctly, leading to an incident being logged and must detect Events to analyse and then determine the appropriate control activity or action to prevent an Incident and/or service interruption.

6.7 The Contractor shall:

(a) ensure that effective 'Event Management' is in place to:

(i) provide mechanisms for early detection of Incidents and assigning them to the appropriate group for action before any Service Outage occurs;

(ii) make it possible for some types of automated activity to be monitored by exception, thus removing the need for expensive and resource-intensive, real time monitoring, and thereby reduces down time;

(iii) signal, when integrated into other Service Management processes, status changes or exceptions that allow the appropriate person or team to respond promptly, thus improving the performance of the process; and

(iv) provide a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work;

(b) ensure that Events are logged, tracked, filtered, aggregated and associated when they are related in accordance with the 'Event Management' policies and procedures;

(c) investigate and manage across all Services the resolution of exceptional or abnormal Events that have reached a threshold or met certain criteria in accordance with the 'Event Management' policies, processes and procedures and the Authority non-functional requirements as specified Appendix 1 to Annex M of Schedule 2.1 (Non-Functional Requirements & Service Availability); and

(d) create and define automated 'Event Management' interfaces for the 'Event Management System' requiring minimal manual intervention.

Incident Management

6.8 The Contractor acknowledges and understands:

(a) the purpose of the ITIL function of 'Incident Management' is to return the Services to required Performance Indicators as quickly as possible and minimising adverse impact and disruption on normal business operations, at a cost-effective price;

(b) the achievement of 'normal service operation' is dependent on meeting the Non-Functional Requirements as set out in Appendix 1 of Annex M to Schedule 2.1 (Non-Functional Requirements & Service Availability);

(c) the Authority requires Incident Management to be the process that handles all failures, faults or questions reported by End Users, Contractor staff or Authority staff via the Service Desk or automatically detected and reported by Event Management via Monitoring Tools. Incident Management should include the use of Incident Models that include the following steps within the Incident Management lifecycle:

(i) log and categorisation of the Incident;

(ii) diagnosis and the steps required to handle the Incident;

(iii) assign responsibilities for the performance and execution of first-level, second-level and third-level support, analysis, diagnosis and resolution of the incident;

(iv) set expectations on timescales and thresholds for the completion of identified actions;

(v) manage the escalation activities based on pre-defined hierarchy and communication plan;

(vi) identify measures, when appropriate, to minimise future disruptions; and

(vii) manage the end-to-end Incident lifecycle;

(d) effective 'Incident Management' allows the business to continue to realise the benefits of enabling ICT technologies and services by:

(i) minimising downtime of the Services, and where applicable the Services, to the business;

(ii) ensuring Services are aligned with day-to-day business priorities;

(iii) identifying potential service improvements (using the Continual Service Improvement process, which engages with the Authority); and

(iv) identifying additional service or training requirements and reporting these to the Authority.

6.9 The Contractor shall:

(a) ensure that the ITIL 'Incident Management' processes are in place to ensure the restoration of normal service operation as quickly as possible, minimising the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained;

(b) uniquely register all Incidents, complaints from End Users, and escalations and ensure that all are logged and that the information regarding these is retained and auditable for the Term and retained thereafter;

(c) investigate all instances of unavailability within the Service and will undertake a structured Service failure analysis as part of this. Where required, this will include techniques like fault tree analysis to determine the chain of events contributing to the failure in question, and the instigation and implementation of appropriate remedial actions required to resolve all such instances, including any investments required as necessary;

(d) provide their processes and procedures that will be put in place for the investigation, diagnosis and resolution of incidents relating to the Service;

(e) proactively deliver and ensure all incidents are resolved within required Performance Indicators for Incident Management (as set out in Appendix 1 of Annex M to Schedule 2.1 (Non-Functional Requirements & Service Availability));

(f) implement an electronic and automated 'Incident Management' system that supports the 'Incident Management' policies and procedures and make the 'Incident Management' system available to the Authority;

(g) record every Incident, assign a unique reference and track in an auditable 'Incident Management' system the records for each Incident, including (but not limited to) its history, outcome, resolution and closure and make available to the Authority;

(h) not use 'on-hold' or 'clock-stop' facilities for Incident resolution when delivering the ITIL 'Incident Management' processes and functions, unless agreed with the Authority;

(i) ensure that the Incident Management process provides an audit trail that complies with the Incident Management policies and procedures relating to the management and resolution of Incidents, including (but not limited to):

(i) records of all detailed audit information pertaining to each Incident; and

(ii) end-to-end traceability for each Incident. All information added to the Incident Report must be preserved within the integrated Service management tool.

(j) ensure that Incidents are monitored, progressed and resolved in required time limits in accordance with the Performance Indicators of the Authority (as set out in Appendix 2 of Annex M to Schedule 2.1 (Incident Resolution Matrix));

(k) for any new Incident that is related to an existing Incident or Problem, ensure aggregation and reference linkage in adherence to the Incident and Problem Management Policies, Procedures and the integrated Service management tool;

(l) ensure that full and complete information about the status of all Incidents is made available to the Authority, via the integrated 'Service Management' tool;

(m) ensure that an Incident record is assigned a closed status in the 'Incident Management' system only upon appropriate verification from the either party raising the initial incident, or the nominated party authorised to confirm closure, that the Incident has been resolved and the Service has been restored in line with the Incident Management Policies and Procedures;

(n) update the Incident record in a timely and accurate manner, with all relevant information relating to the Incident;

(o) adhere to the Severity and Priority definitions in accordance with Priority Levels as specified in this Agreement;

(p) have a process in place to manage any major Incidents including initial notification, regular progress updates, resolution notification and final closure notification to the relevant Authority individuals via email, SMS/text and phone;

(q) perform a detailed analysis of the reasons and handling of any major incident and provide a report to the Authority including lessons learnt and any changes to be implemented from the findings, no later than 1 month from Incident closure;

(r) monitor on a regular basis any actions identified as part of the major Incident review and report progress to the Authority as part of the Service Review meetings;

(s) carry out Incident analysis to determine the categorisation, Priority Level and assignment of an Incident to the appropriate Resolver Group in accordance with the 'Incident Management' policies and procedures and the SKMS (as set out in Schedule 8.2 (Change Control));

(t) define the allocation rules which must be used by the Service Desk to allocate Incidents to the appropriate Resolver Groups and must record these in the Incident Management policies and procedures;

(u) ensure that Resolver Group carries out escalation of all open Incidents that it is unable to resolve itself (which shall consist of the routing of the Incident to the correct member of the Resolver Group);

(v) monitor Incident volumes and report to the Authority, at agreed intervals, on such volumes providing trend analysis relating to the Incidents raised over the past Service Period, quarterly and annual (including year to date) profiling. Such reports to the Authority to include (but not be limited to):

(i) the number of Incidents;

(ii) the source of Incidents;

(iii) the type and category of Incidents;

(iv) the length of time for open Incidents (overall averages and volumes by age);

(v) the number of Incidents resolved including those resolved by first contact at the Service Desk;

(vi) key issues relating to Incident Management;

(vii) the volume of Incidents during the period by Priority/Severity, service, Authority stakeholders (being those parties involved in the process) and/or classification;

(viii) a cross-reference with identified Problem records;

(ix) Incident fault location;

(x) initial fault diagnosis;

(xi) initial Resolver Group allocation; and

(xii) ultimate Resolver Group;

(w) change the assigned Priority Level of an Incident, to align the Incident with the correct Priority Level where appropriate or when required to do so by the Authority;

(x) provide formal training on the use of the 'Incident Management' system to the Authority;

(y) provide access to the 'Incident Management' system to the Authority at all times; and

(z) notify the Authority (Tech Assurance) of any Incident to Services that is known to be in breach or highly likely to breach its Performance Indicators within 1 hour of the incident occurring.

Problem Management

6.10 The Contractor acknowledges and understands that the ITIL process of 'Problem Management' deals with the underlying causes of incidents; the functionality of 'Problem

Records' should be similar to those needed for Incident Records and also allow for multiple incidents matching against Problem Records; the principle objective of 'Problem Management' is to prevent Problems from occurring by eliminating recurring Incidents and to minimise the impact of Incidents that cannot be prevented; and this service must include the following steps in the 'Problem Management' lifecycle:

(a) detection of Problems;

(b) capture and categorisation of Problems;

(c) investigation and diagnosis of Problems; and

(d) resolution of Problems,

which must seek to:

(e) reduce the number of Incidents raised across the Services;

(f) use 'Root Cause Analysis' to determine cause of Problems and to further eliminate potential issues;

(g) implement a permanent fix for all identified problem causes; and

(h) log and maintain known errors and workarounds to prevent Service Outage.

6.11 The Contractor shall:

(a) implement a 'Problem Management' system that supports the 'Problem Management' policies and procedures and must make the 'Problem Management' system available to the Authority;

(b) ensure that all Problems are logged in the 'Problem Management' system using a unique sequential reference;

(c) ensure that Problems are assigned to the appropriate Resolver Groups;

(d) ensure that problem control processes identify the root cause of incidents and report it to the service desk and handle problems in an efficient way;

(e) ensure that other activities include Problem identification and recording, Problem classification, Problem investigation and diagnosis;

(f) adopt standardised and structured root-cause analysis methods to develop a thorough understanding of the problem and its causes, identify corrective/preventive actions that will reduce the risk of recurrence to an acceptable level;

(g) independent on the outcome of the root cause analysis, instigate remedial action including raising any relevant Change Authorisation Notes;

(h) ensure that problem management processes and measures are in place to resolve the root causes of incidents and thus to minimise the adverse impact of incidents caused by errors across the Contractor Systems, and to prevent recurrence of incidents related to these errors;

(i) deploy processes that include error control, trend analysis, targeting support action, and providing information to the Authority. The error control process must iteratively diagnose known errors until they are eliminated by the successful implementation of a change under the control of the Change Management process;

(j) ensure that Problems are monitored and progressed in line with the Performance Indicators required by the Authority;

(k) own and manage the resolution of Problems;

(l) provide Problem analysis to the Authority, including (but not limited to) information relating to Problem trends, volumes, and Problem solutions;

(m) provide the following Problem information for all Authority Systems and associated Software and Applications, broken down by for each Software instance and application, including (but not limited to):

(i) total number of Problems reported for that month;

(ii) total number of Problems resolved for the reported month;

(iii) total number of Problems outstanding;

(iv) total number of Service Outages for the previous Service Period and the duration of each outage; and

(v) the cumulative total of the duration of the Service Outages for the previous 12 month period;

(n) provide problem management reporting to the Authority, including (but not limited to):

(i) common terms, language, and structure with respect to root cause analysis;

(ii) clear and concise problem identification, including actual and potential impact;

(iii) identification of the problem's causes, their interactions, and the supporting evidence;

(iv) identification of corrective / preventive actions that will prevent recurrence of the problem; and

(v) development of a knowledge base which others can use as a resource;

(o) monitor and report on the resolution of Problems across the Service and ensure their resolution in accordance with the Problem Management policies and procedures;

(p) prioritise Problem solution in accordance with the level of business impact and urgency identified by the Authority and in accordance with the Problem Management policies and procedures;

(q) organise, facilitate and lead Problem reviews with the Authority, as required and in accordance with the Problem Management policies and procedures;

(r) manage, co-ordinate and communicate responses to the Authority's End User community on the status of Problems in accordance with the Problem Management policies and procedures; and

(s) manage the reduction of Incidents and Problems through continual improvement of the Problem Management policies and processes.

Request Fulfilment

6.12 The Contractor acknowledges and understands that the ITIL process of 'Request Fulfilment' is the process for managing Authority's Service Requests that are standard and repeatable changes initiated via an automated catalogue of Services and follows the steps within the 'Request Fulfilment' lifecycle. To deliver a 'Request Fulfilment' process that enables Authority staff to receive Services available from the Service Catalogue by providing the ability to, the Contractor is required to:

(a) source and supply requests made, delivering the requested service to the Authority;

(b) provide information to Authority about the Services on offer and the process and procedures to be followed to obtain them;

(c) support the Authority with general information requests, complaints other general comments;

(d) capture, log and track all requests and providing status information on requests submitted; and

(e) control the distribution and consumption of Services through the use of appropriate approval and validation methods to requests before they are fulfilled.

6.13 The Contractor shall:

(a) manage and coordinate via the Service Desk the Request Fulfilment process and manage the achievement of Performance Indicators;

(b) provide a simple-to-use portal for Authority staff to log Service Requests for a Service from the Service Catalogue;

(c) assign each Service Request to the appropriate resources in accordance with the Request Fulfilment Policies and Procedures;

(d) proactively manage and monitor the status and progress of all Service Requests across the Services ordered via the Services Catalogue;

(e) respond to the Authority's enquiries according to the required response times of requests regarding Authority Service Requests with accurate and up-to-date information;

(f) provide early notification of any potential breach of Performance Indicators relating to Service Requests to the requesting Authority resource;

(g) ensure Request Fulfilment or request management processes ensure that Service Requests, which will include minor standard changes (for example, requests to change a password or requests for information), are completed within required timescales to required quality;

(h) provide a channel for Authority staff to request and receive standard Services for which a pre-defined approval and qualification process exists;

(i) receive, record and maintain logs of all Service Requests;

(j) be obliged to deliver in line with the priority that the request was logged with;

(k) ensure that Requests are treated in the same way as any other Service Desk call;

(l) assign the Request to the appropriate support team or Third-Party Contractor to satisfy the request. The Contractor may vary the priority of the Service Request only with agreement from The Authority;

(m) assign the Standard Request to the appropriate support team to satisfy and fulfil the Request;

(n) at either the Contractor's or the Authority's request, if it is reasonable to do so, ensure that sets of like or related Service Requests may be aggregated and a Request for Change requested;

(o) process all Requests to the agreed Performance Indicators;

(p) monitor the progress of the Request and inform the Authority resource requesting the status of the Request;

(q) ensure that the Contractor Service Desk updates the progress of all Requests and the Contractor must monitor the progress of the Request and must inform the Authority resource whenever there is any deviation from the agreed timescale;

(r) close Service Requests following acceptance by the Authority requesting the Request that the Requirements have been satisfied;

(s) ensure that the Contractor's Service Desk must inform the End User that the Service Request has been completed. If they are satisfied, the Contractor will also close the request on their system; and

(t) monitor, analyse and report on Service Requests, including (but not limited to) volumes, trends, and categories within each Service Period.

Service Desk

6.14 The Contractor acknowledges and understands that the ITIL function of 'Service Desk' is a vitally important part of any organisation's ICT and business service which must offer value to the Authority by ensuring effective and timely management of Service Events and for specific business processing services related to the core Service provisions required to provide a single unified capability for each element of the Service and any ICT issues related to the Service provision.

6.15 The Contractor shall provide a single English-speaking 'Service Desk' as a single point of contact for all Contractor and Authority staff to raise issues related to the Services which shall;

(a) adhere to the specific Authority business process requirements across Mil Pers & Vets, as detailed in Annex K (Contact Centre, Help Desk & Telephony) and Annex D (Pensions and Compensation);

(b) be used for the recording and managing of all automatically generated or Contractor raised issues related to the service, so that there is a single source for all incidents and issues affecting the Service;

(c) provide a consistent and effective 'Service Desk' toolset for managing and reporting all interactions with the Authority and End Users;

(d) be capable of the handling Incidents, Problems, questions and requests and manage the end-to-end life-cycle management of all service requests and communication, keeping the Authority informed of progress and outcomes;

(e) provide an interface for other ITSM processes contained in this Appendix;

(f) provide a flexible resourcing model supporting the Authority's patterns of business activity;

(g) proactively monitor, investigate and escalate Incidents, Service Requests to other Resolver Groups, communicating any potential failures to meet the Performance Indicators;

(h) provide, maintain and publish to the Authority up-to-date contact details for the Service Desk in accordance with the Service Desk policies and procedures, including (but not limited to):

(i) how to contact the Service Desk;

(ii) options for accessing the Services Desk;

(iii) service hours;

(iv) the scope of the Service Desk services; and

(v) response times;

(i) accept contact from the Authority and its End Users via either telephone, email, Contractor-hosted self-service portal and any other agreed channels;

(j) actively seek to develop and provide alternative methods in delivering the self-service facilities in support of the provision and consumption of Service Desk services (to be implemented on the Authority's prior written approval);

(k) ensure that the Service Desk uses information supplied by the 'Incident Management' system, the Service Knowledge Management System and the Problem database to conduct an initial Incident analysis and must resolve as a first point of contact whenever possible;

(l) ensure that all Service Desk staff have access to the Service Knowledge Management System;

(m) where necessary, provide appropriate training in the use of the Service Desk for 'Incident Management', 'Problem Management', 'Service Request' and 'Service Knowledge Management' to the personnel of the Authority who interact with the Service Desk; and

(n) update and communicate status updates to the End User on Incident and Service Request as defined in the Service Desk policies and procedures.

7 CONTINUAL SERVICE IMPROVEMENT

7.1 The Contractor acknowledges and understands that the purpose of the ITIL process of 'Continual Service Improvement' is to create and maintain value in the design, introduction, operation and use of Services through the process of 'Plan', 'Do', 'Check', 'Act', 'Service Improvement Plans' are created based on shortfalls or opportunities identified; the primary purpose of 'Continual Service Improvement' is to continually align and realign the Services to the changing Authority needs by identifying and implementing improvements to Services that support the Authority's core business. Improvement activities must support the lifecycle approach through Service Strategy, Service Design, Service Change and Service Operation.

7.2 The Contractor shall provide the ITIL 'Continual Service Improvement' service in accordance with Clause 8 (Service Improvement) which includes the following steps in the 'Continual Service Improvement' lifecycle:

(a) reviewing management information and trends to ensure that services are meeting agreed Performance Indicators;

(b) reviewing management information and trends to ensure that the output of the enabling ITSM processes are achieving the desired results;

(c) periodically conducting maturity assessments against the process activities and roles associated with the process activities to demonstrate areas of improvement or, conversely, areas of concern;

(d) periodically conducting audits verifying employee and process compliance;

(e) reviewing the Services for improvements;

(f) making recommendations for approval; and

(g) conducting periodic Authority satisfaction surveys.

7.3 The Contractor shall:

(a) ensure that Continual Service Improvement is structured to provide Service performance reporting and measurements which adhere to the requirements as set out in Schedule 2.2 (Performance Levels);

(b) produce, maintain and provide a Service Improvement Plan which incorporates the elements established in this section of the schedule and submit it to the Authority for approval;

(c) ensure that it effectively discharges its obligations set out in the relevant Service Improvement Plans to ensure that such Service Improvement Plans are implemented effectively in accordance with the Continual Service Improvement policies and procedures in the Service Operation Manual;

(d) ensure that the Continual Service Improvement programme aligns to the fullest extent possible with the priorities that have been assigned to Service Improvement Plans by the Authority;

(e) keep the Authority informed on the progress against Service Improvement Plans, by means of a quarterly report;

(f) implement deliver and maintain Service and performance measurement processes;

(g) support the Authority to develop a strategy for Service measurement and performance;

(h) ensure that Service measurement and performance is developed and aligned with the Authority's strategic ICT objectives;

(i) instigate a process of identifying any improvements to Service measurement and performance in accordance with the Continual Service Improvement service;

(j) ensure that the service includes the following steps in the Service Measurement and Performance Management lifecycle:

(i) design of a Service Measurement and Performance framework;

(ii) design the Service Reporting Framework;

(iii) identification of appropriate measurements; and

(iv) production, distribution and publication of reports;

(k) ensure that the reporting process produces factual evidence and / or demonstrable proof to support and enable effective decision making;

(l) ensure that the service measurement and performance processes use a reporting process that contains measurements that are 'SMART' (specific, measurable, attainable, realistic, and time-bound);

(m) provide a performance monitoring framework capable of providing different perspectives supporting, including (but not limited to):

(i) the use of a monthly Balance Scorecard showing a mixture of quantitative and qualitative measures;

(ii) the differing requirements of the Authority's user profile;

(iii) presents IT control performance information to industry standards (for example, COBIT);

(iv) viewable data by the Authority's stakeholders (i.e. parties involved in the processes), the Service consumed by such stakeholders, End User and/or site/location; and

(v) sufficient granularity to identify the effects of poor performance and implemented service improvements;

(n) provide performance information that informs the Authority to the extent that:

(i) enables evaluation of performance of Services against Performance Indicators, Authority objectives, and other agreed performance measures; and

(ii) enables comparison analysis of Service performance against past, present and forecast of future predictions;

(o) ensure that performance information is defined in a structured and rigorous way to facilitate automation of acquisition, exchange and quality management. Such performance information shall include (but not limited to) details of:

(i) performance over the agreed Service Reporting Period;

(ii) year to date (over 18 month rolling period); and

(iii) show an aggregate of performance month on month over an 18 month period;

(p) manage Performance information quality by ensuring that the quality of source information for performance is complete, accurate and timely; and

(q) ensure that CSI is planned and scheduled as a process with defined activities, inputs, outputs, roles and reporting.