We released this document in response to a Freedom of Information request. Over time it may become out of date.

Department for Work and Pensions

SCHEDULE 2

SERVICES

1 Purpose of this Schedule

1.1 This Schedule, including its Annex, details the Services that shall be provided by the CONTRACTOR pursuant to this Agreement.

1.2 General

(a) In providing the Services under this Agreement, the CONTRACTOR shall provide continuity of service to the AUTHORITY across areas including but not limited to:

(i) Service Desk Services;

(ii) Application Support Services;

(iii) Infrastructure Support Services;

(iv) Project Management Services;

(v) development, testing and implementation of new and changed Service Builds;

(vi) Service Delivery and Service Support Information Technology Infrastructure Library (ITIL) functions;

(vii) Disaster Recovery Services as defined in Schedule 5 (Disaster Recovery);

(viii) Network Operations Centre (NOC) Services as defined in Annex A to this Schedule 2 (Services);

(ix) Hosting Services as defined in Annex A to this Schedule 2 (Services);

(x) Security Management;

(xi) Application Development;

(xii) Operational Acceptance Testing;

(xiii) Technical Design;

(xiv) Third Party Management; and

(xv) Continuous Improvement Programme (CIP).

(b) In performing the Services under this Agreement, the CONTRACTOR shall ensure and provide:

(i) continued security accreditation;

(ii) sufficient flexibility to respond to changing business needs, such as changes in Service Levels;

(iii) maintenance, development and improvements to the quality of information provided to the AUTHORITY and its availability to managers and their staff;

(iv) the ongoing enhancement of supporting infrastructure, applications, processes and tools;

(v) Service improvement during the lifetime of the Agreement;

(vi) ongoing improvement to availability levels of the Gateway;

(vii) technical design to specify the infrastructure, application standards and software in order to ensure compatibility, interoperability and adherence to known and emerging government standards and initiatives;

(viii) scalability to support agreed increases in take-up of the Gateway including effecting changes, when appropriate, in accordance with the Change Control Procedure;

(ix) an incremental approach to the development of the infrastructure and applications;

(x) the capacity to deliver new applications to meet changing business needs; and

(xi) that the long term strategic direction is not compromised.

(c) The CONTRACTOR shall ensure that all elements of the provision of the Services are co-ordinated to achieve seamless and effective delivery of the Services.

(d) The Services shall support inter-working and collaboration between the AUTHORITY and other public sector organisations.

(e) The Services, are based around a number of guiding concepts as set out in sub-paragraphs (i) to (iv) below. These concepts set out the principles for how the CONTRACTOR must deliver the Services and such concepts and principles shall be extended in consultation with the AUTHORITY throughout the lifetime of this Agreement. The principles are as described below:

(i) Although Service Levels are given in Schedule 4 (KPIs, Service Levels and Service Credits), the AUTHORITY expects that the quality and scope of Services delivered will undergo improvement throughout the duration of this Agreement through the Continuous Improvement Programme, in accordance with Schedule 6 (Continuous Improvement Programme).

(ii) The AUTHORITY’s requirements for its technical infrastructure are subject to change, just as the AUTHORITY is subject to changes in the approach taken by Government to the provision of e-services. The delivery of Services to meet the needs of the AUTHORITY must therefore be readily adaptable to these changes, allowing the AUTHORITY to be flexible in its approach. Changes will be effected in accordance with Schedule 24 (Change Control) .

(iii) The CONTRACTOR will deliver the infrastructure and application capability covered by this Agreement to meet the needs of the AUTHORITY's Customers, however the relationship with the AUTHORITY's Customers will always be managed and controlled by the AUTHORITY, unless such responsibility is otherwise granted to the CONTRACTOR by the AUTHORITY.

(iv) The AUTHORITY ICT environment is delivered by a number of different service providers. The CONTRACTOR will work efficiently and effectively with other service providers including where reasonable the AUTHORITY's Customers, to achieve the successful delivery of the Services.

(f) The Services shall be delivered, managed and measured based on the agreed standards set out in Schedule 4 (KPIs, Service Levels and Service Credits) and the principles of a set of Best Practices applicable to achieve the most effective Services. This shall be determined by acknowledged industry Best Practice, which shall be based on but not limited to:

(i) ISO 9000:2000;

(ii) ISO20000;

(iii) ISO17799 & BS7799;

(iv) ITIL recommendations;

(v) payment industry recommendations and accreditation requirements; and

(vi) other methodologies and / or principles of Best Practice where they offer specific benefit to the Services.

(g) Best Practice shall be further judged against the following attributes:

(i) the Services underpin the business needs;

(ii) service delivery is process orientated;

(iii) processes are integrated and automated where appropriate;

(iv) processes are documented, current and completed within a timely manner;

(v) processes are repeatable; and

(vi) processes are measurable.

(h) Evidence of Best Practice service delivery shall be accepted through current certification, certification planning and/or benchmarking assessment in accordance with Schedule 9 (Benchmarking). The objective shall be to determine suitability, integration (where appropriate), quality, effectiveness and efficiency of the following:

(i) processes;

(ii) Service Management tools;

(iii) Documentation;

(iv) Customer satisfaction; and

(v) quality of ongoing service.

(i) The AUTHORITY shall during the Transition project provide the CONTRACTOR with the names of authorised individuals who are permitted to request and authorise Service Requests and Change Requests for the Service on behalf of the AUTHORITY in accordance with the procedure agreed with the AUTHORITY and set out in Schedule 2 (Services) and Schedule 24 (Change Control).

(j) The AUTHORITY will use reasonable endeavours:

(i) to assist the CONTRACTOR in the timely notification to Users of changes to Services; and

(ii) in conjunction with the CONTRACTOR, ensure that the AUTHORITY's Customer(s) have access to relevant documentation and information in the format reasonably required by the AUTHORITY to allow them to use the Services properly, effectively and efficiently;

(k) Any AUTHORITY employees or third parties to the AUTHORITY made available to assist the CONTRACTOR in its provision of the Services shall, be made available on a free of charge basis, unless, following consultation with the CONTRACTOR, they are made available to assist the CONTRACTOR in rectifying any default by the CONTRACTOR.

(l) The AUTHORITY's Customers are responsible for:

(i) their own links and interfaces to the Government Gateway Services;

(ii) the content of their Data (other than degradation or unauthorised alteration of such content caused by a failure of the CONTRACTOR to perform its obligations under this Schedule 2 (Services);

(m) The AUTHORITY will advise the CONTRACTOR of any "special needs" relating to the use of the Gateway by disabled persons which require a change to the Services which shall be performed in accordance with Schedule 24 (Change Control).

(n) Application Support

(i) The CONTRACTOR will not provide Problem Resolution for the AUTHORITY's Customer(s) non Gateway application issues. Where Problem diagnosis by the CONTRACTOR indicates that there is no known issue with the Gateway related to the issue raised, then the responsibility will be passed back to the AUTHORITY's Customer to demonstrate that their non Gateway application is or is not functioning correctly before the CONTRACTOR will take any further action on such new Incidents.

(o) The CONTRACTOR will draw up guidelines for the use of the Gateway Environment(s) by the AUTHORITY's Customer(s). On AUTHORITY agreement of these guidelines both Parties will seek to ensure that the AUTHORITY's Customer(s) abide by these guidelines.

(p) The AUTHORITY and the CONTRACTOR will use reasonable endeavours to encourage the AUTHORITY's Customer(s) to update their back-end systems / applications to make use of the existing Gateway automated method for uploading Known Facts.

2 Scope Of Services

2.1 The CONTRACTOR will provide:

(a) a Managed Service as described in paragraphs 3, 6, 7 and 10:

(i) to manage the operation and support of the Gateway and its associated services and sub-contracts;

(ii) overall escalation processes as described in paragraph 4;

(iii) overall controls and procedures as described in paragraph 5;

(b) Service Builds as described in paragraph 8;

(c) an Application Development Service as described in paragraph 9 to meet Gateway functionality requirements agreed with the AUTHORITY;

(d) a Core Committed Team as described and defined in paragraph 12; and

(e) Ad-Hoc Projects Services as described in paragraph 13 to deliver ad-hoc requirements.

2.2 For each service requirement within Application Development and Ad-Hoc Project Services, the CONTRACTOR shall provide the Services in accordance with the delivery timescales and technical specification agreed with the AUTHORITY.

2.3 The CONTRACTOR shall provide the following functions for the Gateway ("Gateway Functions") set out as follows:

(a) Registration & Enrolment Engine (R&E)

A pan-Government facility that allows citizens, organisations and agents to register and enrol for multiple government services. This is done by the User providing a set of 'Known Facts' about themselves or the organisation which are known to a Customer.

(b) Authentication Engine

A pan-Government facility that allows citizens, organisations, agents, government individuals and government organisations to securely authenticate for multiple Government services. This is done by the User providing trusted credentials such as User ID and password or a digital certificate.

(c) Transaction Engine (TxE)

A pan-Government facility that allows citizens, organisations and agents to securely submit online forms to government, and for Government bodies to communicate asynchronously. The Gateway Transaction Engine reliably sends the submission to the relevant Government system for processing and returns an appropriate validation and/or confirmation message to the User or Government body.

(d) Help Desk Tools Application

A pan-Government facility used by Customer helpdesk operators to carry out various duties and enquiries in support of the Customer's business through the Gateway. The Help Desk Tools Application queries the Gateway and is accessed through a browser via either the GSI or a secure Internet connection.

(e) Payments Engine

A pan-Government facility that provides the connectivity to enables Government bodies to connect to the merchant acquirer of their choice for the processing of on-line payments and refunds.

(f) Secure Mail

A pan-Government facility that enables secure outbound communication between an AUTHORITY Customer and a User.

(g) Alerts Engine

A pan-Government 'opt in' facility that provides SMS and email messaging to citizens, organisations and agents.

(h) Secure Printing Services

A service that produces printed Gateway credentials including Gateway IDs, passwords and activation PINS that are required for citizens, organisations and agents to either complete registration and enrolment or to authenticate on the Gateway.

(i) Secure Posting Services

A service that ensures timely delivery of printed Gateway credentials to citizens, organisations and agents.

2.4 The AUTHORITY shall provide such staff as required who will have such knowledge of the AUTHORITY's organisation, operations and business practices as is appropriate for the activities to which they are assigned.

3 User Support

3.1 Service Desk

(a) The CONTRACTOR shall provide a Best Practice Service Desk based on but not limited to ITIL, operating on a 24*7 basis.

(b) The CONTRACTOR shall provide dedicated Service Desk staff from 07:00 to 23:00, and at other times calls will be handled by NOC staff.

(c) The CONTRACTOR shall provide infrastructure and application support staff from 08:00 to 18:00 Monday to Friday, with an on-call service out of these hours for P1 Incidents and P2 Incidents for the Production Environment.

(d) The CONTRACTOR shall provide a Service Desk facility to deal with all 2nd level technical enquiries from the AUTHORITY and to be the central point of contact to receive all Incidents, Change Requests and Service Requests.

(e) The Service Desk facility shall deal with the following channels of requests or enquiries:

(i) telephone calls;

(ii) e-mail;

(iii) Internet sourced ("self-serve"); and

(iv) any other channels as mutually agreed between the Parties.

(f) The CONTRACTOR must ensure that queries and requests regardless of the source channel will be dealt with equal priority and within the same ITIL process and will allow for multiple channels within the same overall communication process (e.g. telephone and e-mail).

(g) All contacts with the Service Desk must be appropriately logged, regardless of whether these result in an Incident or Service Request.

(h) The functions of the CONTRACTOR's Service Desk are:

(i) providing an operational interface between the AUTHORITY, the AUTHORITY's Customer and the service provider(s) to resolve daily Incidents and Service Requests as they occur;

(ii) prioritisation of Incidents and Service Requests according to pre-set criteria;

(iii) providing primary contact for daily operational Incidents, Service Requests and Change Requests;

(iv) providing 1st level support and routing to 2nd level support for Incidents and Service Requests;

(v) provision of 2nd level support and routing to third line support for Incidents and Service Requests;

(vi) logging and tracking calls into the Service Desk through to Resolution, including a timetable for any support actions from receipt;

(vii) resolving minor Incidents or Service Requests;

(viii) routing other Incidents to the appropriate resource for Resolution;

(ix) escalating critical Incidents according to an agreed Escalation Procedure;

(x) ensuring the AUTHORITY's Customer(s) are updated throughout the life cycle of a call in accordance with agreed Service Levels;

(xi) informing the AUTHORITY's Customer(s) of Resolution details for all calls logged;

(xii) confirming call closure with the AUTHORITY's Customer(s) in accordance with agreed processes;

(xiii) providing classification of call upon closure for reporting purposes;

(xiv) inform the AUTHORITY and the nominated AUTHORITY's Customer contacts of any Priority 1 & 2 Incidents;

(xv) informing the relevant representative of the AUTHORITY in advance if the CONTRACTOR can anticipate that an Incident will have a major impact on the Services;

(xvi) managing the timely and accurate allocation, ownership and monitoring of Service Requests to completion (including request for information); and

(xvii) managing Change Requests as described in Schedule 24 (Change Control).

(i) The CONTRACTOR shall provide a call out service to manage Priority 1 & 2 Incidents that are affecting the AUTHORITY and/or the AUTHORITY's Customer(s) and to allow for the invocation of disaster recovery plans in event of a disaster. The CONTRACTOR shall provide a method for contacting 2nd and 3rd line support out of hours.

(j) The AUTHORITY will use reasonable endeavours to ensure that the AUTHORITY's Customer(s) notify any faults, Incidents, Change Requests and Service Requests to the Service Desk using agreed procedures and where the AUTHORITY's Customer notifies the AUTHORITY directly the AUTHORITY shall either:

(i) notify the Service Desk; or

(ii) direct the AUTHORITY's Customer to notify the Service Desk.

Any Incidents, Change Requests or Service Requests not notified in accordance with paragraph 3.2(b) shall be excluded from Service Level calculations.

3.2 Incident Management

(a) The CONTRACTOR shall provide an end-to-end Incident Management Service for all areas of the Gateway and the Services, on all Gateway Environments**.** The facilities provided by the Incident Management Service are:

(i) timely Incident detection and recording;

(ii) accurate classification and initial investigation;

(iii) timely and accurate allocation of Incidents;

(iv) ownership and monitoring of all Incidents through to successful Resolution;

(v) ensuring all updates are recorded and communicated to the AUTHORITY's Customer(s) in a timely manner;

(vi) allocating to multiple support teams for parallel investigation where required and co-ordinating any joint investigations between support teams;

(vii) manual and automatic escalations throughout the Incident lifecycle to the point of Resolution and closure; and

(viii) liaison with specific service providers (e.g. Dell) in relation to services provided by them and with the AUTHORITY with respect to business issues outside of the CONTRACTOR's scope.

(b) Where a call is not the subject of an earlier call from a different AUTHORITY Customer(s), the CONTRACTOR shall:

(i) enter the Incident into the CONTRACTOR's Incident Management system;

(ii) provide a unique call reference for the Incident;

(iii) assign the Incident a Priority;

(iv) classify the Incident according to initial diagnosis;

(v) manage the Incident through to successful Resolution; and

(vi) where it is a Priority 1 or 2 Incident, inform the AUTHORITY of the nature of the Incident and the scope of the AUTHORITY's Customer(s) affected. Regular updates on the status of the Incident shall then be provided to the AUTHORITY until Resolution, through agreed communication channels which may include SMS, e-mail and telephony.

(c) If the AUTHORITY does not agree with the Priority assigned to the Incident, it will notify the CONTRACTOR of its claimed Priority for the Incident promptly, in writing or by e-mail. Any dispute as to the Priority of an Incident will be escalated in accordance with the agreed Escalation Procedures.

(d) If the call is the subject of a prior call by a different AUTHORITY's Customer(s), the CONTRACTOR shall:

(i) provide the call reference to the AUTHORITY's Customer(s) for the relevant Incident;

(ii) log the call in the Incident Management system; and

(iii) associate the Incident ticket with the "parent" ticket.

(e) Service Levels are measured from the point of when the first ticket is logged within the CONTRACTOR's Service Desk system.

(f) A Clock Stop shall occur in a respect of an Incident:

(i) where the Incident is passed to a third party that is neither a Subcontractor of the CONTRACTOR nor a supplier of services within the scope of the CONTRACTOR's responsibility;

(ii) where the CONTRACTOR is awaiting a response from the AUTHORITY or the AUTHORITY's Customer where there is a clear dependency to progress the Incident;

(iii) where control of the Incident is passed to the AUTHORITY (including in respect of call closure);

(iv) where relevant to the Resolution of the Incident the AUTHORITY's Customer(s) affected by the Incident cannot be contacted by the CONTRACTOR; or

(v) by mutual agreement with the AUTHORITY.

(g) The AUTHORITY's Customer(s) affected will only be considered to be uncontactable where all of the following have been attempted:

(i) the CONTRACTOR has attempted to call the AUTHORITY’s Customer(s) twice and left a message on each occasion where able; and

(ii) the CONTRACTOR has sent an e-mail to the AUTHORITY’s Customer(s).

(h) A Clock Stop shall also be considered to occur in respect of all Incidents for any period of agreed scheduled downtime on that application or piece of infrastructure.

(i) The CONTRACTOR’s obligations to resolve an Incident within the target Resolution time shall be suspended for any period of Clock Stop.

(j) Call closure shall occur in respect of an Incident where:

(i) the CONTRACTOR believes the Incident to be resolved and the requestor or the AUTHORITY has agreed to closure;

(ii) the CONTRACTOR believes the Incident to be resolved, the affected AUTHORITY Customer(s) cannot be contacted and the CONTRACTOR agrees with the AUTHORITY that the call can be closed;

(iii) the CONTRACTOR believes the Incident to be resolved, the affected AUTHORITY’s Customer(s) is uncontactable and has not responded to an e-mail from the Service Desk within 24 hours elapsed time during Standard Working Hours;

(iv) another procedure has been agreed between the CONTRACTOR and the AUTHORITY for call closure;

(v) the CONTRACTOR has passed the Incident back to the AUTHORITY’s Customer(s) for further information and this has not been provided after a period of ten (10) Working Days during which time Clock Stop shall occur in accordance with paragraphs 3.2(f) and 3.2(h);

(vi) the CONTRACTOR has passed the Incident with the Status ‘Solved’ back to the AUTHORITY’s Customer(s) for confirmation to ‘Close’ the Incident and this has not been provided after a period of ten (10) Working Days during which time Clock Stop shall occur in accordance with paragraphs 3.2(f) and 3.2(h).

3.3 Problem Management

(a) The CONTRACTOR shall provide a Problem Management Service to the AUTHORITY in accordance with the features set out below. This Service is designed to improve the delivery of Services by ensuring the Resolution of Problems and identifying trends that may impact on future performance. The features of this Service are:

(i) identify, record and classify Problems;

(ii) prioritisation of Problem based on impact to Service Levels and KPIs as defined in Schedule 4 (KPIs, Service Levels and Service Credits) and the probability of reoccurrence;

(iii) manage the investigation of Problems and coordinate Root Cause Analysis;

(iv) document recommendations;

(v) agree and document follow-up actions, based on recommendations;

(vi) managing the follow-up actions to completion within agreed timescales;

(vii) reporting progress of follow-up actions to the AUTHORITY at regular intervals;

(viii) initiate, complete and present to the AUTHORITY lessons learned reviews, as appropriate;

(ix) evaluate and escalate Incidents that fail to comply with their target Resolution times prior to lessons learned reviews;

(x) co-ordinate and produce Incident review and recommendation reports for the AUTHORITY ensuring follow-up of action items and recommendations (a "Root Cause Analysis");

(xi) analyse Incidents, identify trends and escalate as per the Escalation Procedure as described in paragraph 4; and

(xii) produce management information based on Problem Management data.

(b) This Service is to be used for all Problems affecting delivery of Services to the AUTHORITY.

3.4 Change Management

The CONTRACTOR shall be responsible for Change Management in relation to the Services and shall co-ordinate the Change Requests and Change Request Impact Assessments that relate to the Services, and manage technical change as it affects the Services. Change Management processes shall be undertaken within the principles defined in Schedule 24 (Change Control). Supporting processes shall cover:

(a) Change Control Procedure;

(b) submission, recording and processing of Change Requests;

(c) co-ordination of all Change Request Impact Assessments within the scope of Services;

(d) quality assurance and ensure approval of Change Requests (including management of Change Approval Boards);

(e) scheduling of Change Request implementation;

(f) updating of all relevant documentation;

(g) building, testing and implementation of the solution to support requested Change if applicable ;

(h) monitoring, reporting and closure of Change Requests;

(i) communication to the AUTHORITY's Customer(s); and

(j) management information reporting.

3.5 Release Management

(a) The CONTRACTOR shall be responsible for the management of any and all Releases to any environment used to provide the Services.

(b) The Release Management Service shall provide planning, testing and rollout of all software and hardware Releases and patches to minimise any adverse or unplanned consequences of a Release. User Acceptance Testing (UAT) of any new or amended Services or applications will be the responsibility of the AUTHORITY and the AUTHORITY's Customer(s).

(c) The responsibilities of the CONTRACTOR in providing the Release Management Service include:

(i) planning and overseeing the rollout of software and related hardware, and designing and implementing efficient procedures for the distribution and installation of changes;

(ii) ensuring all relevant Release documentation is produced and accurate;

(iii) ensuring adequate levels of testing are conducted;

(iv) ensuring that security is not compromised as a result of deployment of Releases;

(v) ensuring that tested roll-back plans are documented for all Releases;

(vi) ensuring any change is traceable, secure and that only correct, authorised and tested versions are installed;

(vii) communicating and managing expectations of the AUTHORITY's Customer(s) during the planning and rollout of new Releases; and

(viii) liaising with Change Management to implement new software and/or hardware Releases and to ensure that the CMDB is updated.

(d) A Release may consist of any combination of hardware, services, software, firmware and documents.

(e) The CONTRACTOR shall be responsible for Configuration Management in support of Release Management, which shall cover:

(i) identification of the level of detail required for appropriate management;

(ii) discovery and maintenance of accurate information on Service configurations and their documentation;

(iii) Configurable Items (“CIs”) and Configuration Management Database (“CMDB”) to be based on a logical and clearly defined data model;

(iv) control to ensure that only authorised, identified CIs are accepted and maintained in the CMDB;

(v) status accounting to produce regular status reports on CIs throughout their lifecycle;

(vi) verification and audit to ensure that the actual state configuration matches expected state; and

(vii) roles and responsibilities of relevant stakeholders.

3.6 Configuration Management

(a) The CONTRACTOR shall implement and maintain a CMDB with two main components: the Asset Register, including the Definitive Software Library (DSL).

(b) The Asset configuration information (both hardware & software) made available to the CONTRACTOR during the Transition phase will be used to populate the CMDB in the form of CIs through an implemented interface.

(c) The CONTRACTOR shall implement a DSL, which shall comprise:

(i) a single logical store; and

(ii) a physical file store for the secure storage of bought-in software media.

(d) Configuration Management Database (CMDB)

(i) The CONTRACTOR and the AUTHORITY will agree the CMDB attributes and will ensure the maintenance of a configuration repository for all areas of technical configuration. This repository will encompass:

(A) configuration details of Assets held in the Asset Register;

(B) configuration details of items held within the DSL;

(C) configuration of all applications deployed with the Gateway;

(D) physical storage of up-to-date versions all software installed on Gateway Environments;

(E) identification of other CIs affected when any CI is the subject of an Incident, Problem or Change;

(F) network and configuration and topology;

(G) all Documentation pertaining to the Services;

(H) relationships and dependencies between CIs, that can be easily updated when new CIs are added; and

(I) items as agreed with the AUTHORITY.

(ii) For all CIs, details of both current and historic values shall be maintained by the CONTRACTOR.

(iii) All information held within the CMDB shall be made available for reporting. Summary reports shall be provided to the AUTHORITY at the end of each reporting period.

(iv) The CONTRACTOR shall put in place documented processes for ensuring that changes to CIs are performed in a controlled and managed manner, and in a timely fashion, to ensure the accuracy of all information held in the CMDB.

(e) Asset Register

(i) From the Transfer of Responsibility Date the CONTRACTOR shall maintain a CMDB which shall contain:

(A) network hardware;

(B) network equipment;

(C) infrastructure hardware; and

(D) items as agreed with the AUTHORITY.

(ii) The CONTRACTOR and the AUTHORITY shall agree the definitive Asset attributes to be held in the CMDB which shall include, but not be limited to:

(A) Asset identifier;

(B) location and environment;

(C) manufacturer;

(D) model;

(E) description; and

(F) installation date.

(iii) The CONTRACTOR shall keep a record within the CMDB of all changes to Assets including planned, ongoing and completed changes. These include changes in location, configuration, usage and where the Asset has been subject to a Problem or Incident.

(iv) The CONTRACTOR shall ensure that all information held within the CMDB will be made available for reporting.

(v) The CONTRACTOR shall put in place documented processes for changes to Assets.

(vi) The CONTRACTOR shall perform Asset change in a controlled and managed manner, and in a timely fashion, to ensure the accuracy of all information held in the CMDB.

(f) DSL

(i) From TORD, the CONTRACTOR shall maintain a DSL register of all software in use to provide the Services.

(ii) The CONTRACTOR shall manage and maintain an up-to-date DSL of all software in use within the Gateway. This shall cover:

(A) software product;

(B) software product version;

(C) description of software product;

(D) licence details;

(E) licences held;

(F) date of purchase;

(G) purchase agreement;

(H) software vendor;

(I) supporting vendor;

(J) owner;

(K) system documentation; and

(L) details of escrow arrangements.

(iii) The CONTRACTOR shall record and retain within the DSL all changes to the Gateway and the Services including planned, ongoing and completed changes including changes in location or configuration.

(iv) The CONTRACTOR shall keep a record and retain within the DSL all Problems or Incidents related to the software.

(v) All information held within the DSL shall be made available for reporting.

(vi) The CONTRACTOR shall put in place documented processes to ensure that change to DSL items is performed in a controlled and managed manner, and in a timely fashion, and to ensure the accuracy of all information held in the DSL.

3.7 Availability Management

(a) The CONTRACTOR shall be responsible for providing Availability Management with the objective of optimising capability of the Services to deliver a cost effective and sustained level of availability that underpins the AUTHORITY's business needs as described in Schedule 4 (KPIs, Service Levels and Service Credits). This shall include undertaking ongoing monitoring, measurement and improvement planning for the availability of all aspects of the Services.

(b) Responsibilities of the CONTRACTOR in providing Availability Management relating to the Services are:

(i) optimising Service availability;

(ii) monitoring of service and CIs and exception reporting;

(iii) determining availability requirements in relation to the AUTHORITY's Customer(s) impact;

(iv) predicting and designing for expected levels of availability and security;

(v) producing an availability plan;

(vi) ensuring Service Levels are met by monitoring service availability levels against Service Levels, and monitoring external supplier serviceability achievements;

(vii) collecting, analysing and maintaining availability data;

(viii) producing management Information reporting on the effectiveness and efficiency of the availability management process and which also provides support for other service management processes;

(ix) regularly reviewing and improving Service availability and Configurable Item availability; and

(x) working with the AUTHORITY to agree the schedule for change to minimise maintenance and upgrade time windows.

3.8 Capacity Management and Planning

(a) The CONTRACTOR shall be responsible for the Capacity Management and Planning of the Services including the current and future business requirements of the AUTHORITY's Customer(s), as advised by the

AUTHORITY, ensuring that all current and future capacity and performance aspects of the business requirements of the AUTHORITY's Customer(s) are provided cost effectively. Any necessary or pre-emptive changes shall be in accordance with Schedule 24 (Change Control).

(b) The CONTRACTOR's responsibilities in providing Capacity Management and Planning are:

(i) ensuring that agreed future business requirements for Services are considered, planned and implemented within appropriate timescales;

(ii) understanding and managing the performance of the Services provided to the AUTHORITY's Customer(s);

(iii) managing the scope of Services to ensure that all application and infrastructure resource utilisation is monitored and measured and that collected data is recorded, analysed and reported to the AUTHORITY on a monthly basis;

(iv) analysing utilisation trends within the scope of the Services, including infrastructure and applications, and projecting their potential impact on future known capacity requirements;

(v) producing management information reporting on the effectiveness and efficiency of the capacity management process; and

(vi) ensuring that the prioritisation requirements of the AUTHORITY are included.

3.9 IT Service Continuity Management (ITSCM)

(a) The CONTRACTOR shall be responsible for ITSCM for the Services.

(b) The AUTHORITY shall provide the CONTRACTOR with a copy of the AUTHORITY's Business Continuity Plan and will re-issue the copy whenever the document is subject to change.

(c) The CONTRACTOR shall participate in the AUTHORITY's Business Continuity Management (BCM) for the Gateway as mutually agreed.

(d) The CONTRACTOR shall build and test the ITSCM plan ("ITSCM Plan") no less than 20 Standard Working Days following TORD.

(e) The CONTRACTOR shall review the ITSCM Plan half yearly or after any major changes affecting the recovery plans.

(f) The CONTRACTOR shall test the ITSCM Plan annually.

(g) The CONTRACTOR and the AUTHORITY will mutually agree the test schedule.

(h) The AUTHORITY and the AUTHORITY's Customers will participate in the tests as agreed, at their own cost.

(i) As a minimum, the ITSCM Plan shall describe how the CONTRACTOR shall continue to provide the Services in the event of any identified failures.

(j) The CONTRACTOR shall consider emergency Service Continuity Invocation when a prolonged loss of capability to deliver the Services is expected. The decision to invoke ITSCM Plans shall be taken in conjunction between the CONTRACTOR and the AUTHORITY. The CONTRACTOR shall develop, agree with the AUTHORITY, and implement communication procedures to ensure that the nominated contacts within the AUTHORITY are informed about the possibility of invoking ITSCM Plans.

(k) Disaster Recovery shall be performed in accordance with Schedule 5 (Disaster Recovery).

3.10 Service Level Management

(a) The CONTRACTOR shall:

(i) be responsible for the management of the Service Levels as defined in Schedule 4 (KPIs, Service Levels and Service Credits) for the delivery of the Services;

(ii) maintain and improve the quality of the Services through a constant cycle of agreeing, monitoring, reporting and reviewing Services achievements; and

(iii) instigate actions to eradicate unacceptable performance levels in providing the Service.

(b) The CONTRACTOR's responsibilities for the provision of Service Level Management in relation to the Services are:

(i) measuring and reporting of the Service Levels actually achieved against target as outlined in Schedule 4 (KPIs, Service Levels and Service Credits);

(ii) identification of any potential for improvements to Service Levels in line with business requirements through a continuous improvement programme as defined in Schedule 6 (Continuous Improvement Programme);

(iii) co-ordinating other Service Management and support functions, including Third Party Service Providers; and

(iv) reviewing Service Levels to meet changing business needs or to resolve issues with the Services.

4 Escalation Procedure

4.1 Unless otherwise agreed between the Parties, the following Escalation Procedures shall apply:

(a) All technical issues shall be escalated to the AUTHORITY's Service Delivery Manager and the CONTRACTOR's Operations Manager (or authorised representative/s) for initial resolution, as appropriate.

(b) All security issues shall be escalated to the nominated AUTHORITY and CONTRACTOR Security Managers (or authorised representative/s) for initial resolution, as appropriate.

(c) All related issues with the AUTHORITY's Customer shall be escalated to the AUTHORITY's Service Delivery Manager and/or Business Relationship Manager and the CONTRACTOR's Operations Manager (or authorised representative/s) for initial resolution, as appropriate.

(d) All development issues shall be escalated to the AUTHORITY's Development Manager and the CONTRACTOR's Development Manager (or authorised representative/s) for initial resolution, as appropriate

(e) All other issues shall be escalated to the AUTHORITY's Service Delivery Manager and the CONTRACTOR's Operations Manager.

(f) If appropriate, contractual issues of a routine nature shall be escalated to the AUTHORITY's Contract Manager (or authorised representative/s) and the CONTRACTOR's Account Manager (or authorised representative/s) for initial resolution.

(g) Invoice and payment issues shall be escalated to the AUTHORITY's Contract Manager (or authorised representative/s) and the CONTRACTOR's Programme Director (or authorised representative/s) for initial resolution.

(h) In the event that the Escalation Procedure referenced above does not resolve the issue(s), then escalation is to the next monthly Operations Board. If the Operations Board is scheduled to meet more than seven (7) Working Days in advance then an emergency Operations Board meeting can be called.

4.2 The CONTRACTOR shall:

(a) document further full details of the Escalation Procedures to complement the above as required to perform the Services. All Escalation Procedures shall be mutually agreed by both Parties during the Transition project;

(b) implement the agreed Escalation Procedures; and

(c) record all escalations undertaken in accordance with these Escalation Procedures.

5 Controls and procedures

5.1 All Services performed and procedures used by the CONTRACTOR shall be clearly documented. The documentation shall be published in appropriate form(s) and made readily available to appropriate AUTHORITY personnel or their representatives. Documentation must be at a level that would enable a suitably qualified third party provider to readily take on the Services without major impact on the Gateway.

5.2 All documentation shall be managed, maintained and kept up to date at all times.

5.3 All documentation shall be subject to a formal Change Management process.

5.4 Where a change to a Service or procedure has security relevance the CONTRACTOR must bring the change to the attention of the Security Accreditor and gain approval before the change is implemented. The CONTRACTOR shall promptly provide on request by the AUTHORITY a list of changes that have been considered and implemented.

6 Management Reporting

6.1 During Transition, the AUTHORITY will provide a list of authorised individuals who:

(a) may request reports from the CONTRACTOR.

(b) are to have access to the management systems provided by the CONTRACTOR.

6.2 The CONTRACTOR shall provide all monthly reports electronically to the AUTHORITY by the 8th calendar day of the following month, (or the next Working Day after the 8th calendar day if the 8th calendar day is a non-Working Day).

6.3 The CONTRACTOR shall ensure that all reports are an accurate reflection of the Services performed during the relevant reporting period.

6.4 The final detail and format of these reports shall be finalised by the CONTRACTOR and submitted to the AUTHORITY for approval during Transition. The CONTRACTOR shall make all changes to the proposed format of such reports as reasonably requested by the AUTHORITY and resubmit the report formats to the AUTHORITY prior to TORD.

6.5 In the event that there is a dispute regarding the management reports then this shall be escalated in accordance with the Escalation Procedure.

6.6 The CONTRACTOR shall provide a review of all Service performance as input to the governance boards as described in Schedule 13 (Governance and Reporting).

6.7 The CONTRACTOR shall provide ad-hoc reports based upon the data listed in Paragraph 6.11(a).

6.8 The CONTRACTOR shall receive all requests for ad-hoc reports via the Service Desk.

6.9 The CONTRACTOR shall provide all required reports electronically to the AUTHORITY.

6.10 The CONTRACTOR shall provide all other reports as set out and in accordance with Schedule 13 (Governance & Reporting).

6.11 Standard Reports

(a) The CONTRACTOR shall provide to the AUTHORITY monthly reports including the following information:

(i) performance versus Service Levels;

(ii) performance versus KPIs;

(iii) volumes and trends including, but not limited to:

(A) number of new Service Builds;

(B) number of QPs received;

(iv) business volumes including, but not limited to:

(A) number of submissions (total and successful) by the AUTHORITY's Customers by Service;

(B) number of enrolments (total and active) by the AUTHORITY's Customers by Service;

(C) number of payments and refunds (volume and value) by the AUTHORITY's Customers by Service;

(D) Gateway Authentication Report;

(E) SOAP calls;

(F) number of deployments per type per environment;

(v) Service Desk Metrics including, but not limited to:

(A) number of Problems;

(B) number of AUTHORITY's Customer contacts by channel;

(C) volume of Incidents created by Priority;

(D) volume of Incidents closed by Priority;

(E) number of Change Requests;

(vi) overview of Major Incidents;

(A) Root Cause Analysis for P1 & P2 Incidents;

(vii) overview of changes deployed into Production;

(viii) overview of current usage vs. capacity; and

(ix) overview of Gateway response times.

6.12 Ad-Hoc Reporting

(a) Standard Data

(i) The AUTHORITY will specify:

(A) the exact report requirements; and

(B) the required date upon which the report is required to be delivered.

(ii) The AUTHORITY will give the CONTRACTOR at least five (5) Working Days notice for the report to be produced.

(iii) The CONTRACTOR shall:

(A) assess the requirements for the report; and

(B) notify the AUTHORITY by e-mail of the acceptance of the request or notify the AUTHORITY by e-mail as to why the request cannot be accepted.

(iv) The CONTRACTOR shall accept up to 2 ad-hoc standard data report requests per week.

(b) New Data

(i) The CONTRACTOR shall provide ad-hoc reports in relation to new data.

(ii) The AUTHORITY will specify:

(A) the exact report requirements; and

(B) the required date upon which the report is required to be delivered.

(iii) The AUTHORITY will give the CONTRACTOR at least ten (10) Working Days notice for the report to be produced.

(iv) The CONTRACTOR shall:

(A) assess the requirements for the report;

(B) notify the AUTHORITY by e-mail of the acceptance of the request or notify the AUTHORITY by e-mail as to why the request cannot be accepted.

(v) The CONTRACTOR shall accept up to 2 ad-hoc new data report requests per month.

6.13 Self-service Reporting

(a) The CONTRACTOR shall make available Incident and change data from its USD database for:

(i) standard reports; and

(ii) non-standard reports.

7 System Management Services

7.1 Software Management and Support

(a) The CONTRACTOR shall provide a fully managed Software Management and Support Service for the resident operating systems running on servers managed by the CONTRACTOR, covering all utilised Gateway Environments. The objective of this Service is to maintain the resident operating system on any server based system in good working order and to resolve any faults occurring within the operating system environment. The facilities provided by this Service are:

(i) proactive monitoring of key component systems in order to maximise system availability and reduce system failures;

(ii) management of any hardware or software Incidents arising; and

(iii) generic support of the various components of the operating system.

(b) The CONTRACTOR shall be responsible for:

(i) operating system installation;

(ii) operating system maintenance;

(iii) operating system fixes and patches;

(iv) systems administration;

(v) software installations;

(vi) server management; and

(vii) system documentation.

(c) All vendor recommended service packs and patches to software and hardware shall be applied in a timely manner by the CONTRACTOR.

(d) Unless agreed by the AUTHORITY, all software must be supported by the vendor (e.g. should for example Microsoft cease to support a specific piece of software then this software must be reviewed for replacement or upgrade to a supported version, or replaced).

(e) The CONTRACTOR is responsible for the upgrade of all software used and managed by the CONTRACTOR as and when required. In the event that such upgrades fall outside of the scope of paragraphs 7.1(a) – 7.1(d) above, then these upgrades will be treated and costed as separate Change Requests in accordance with Schedule 24 (Change Control).

(f) The CONTRACTOR is required to schedule preventative maintenance and/or upgrades and to inform the AUTHORITY of the maintenance.

(g) Software must be reviewed for upgrade or replacement when the current Release of the software is greater than two full Releases higher than that used at the AUTHORITY. Software should be reviewed for upgrade if it is more than 3 years old, and at a minimum every 3 years after that.

(h) All software in use at the AUTHORITY must be functionally compatible, ensuring a working and integrated environment.

(i) The CONTRACTOR shall provide systems management to support the operation of the Gateway. The facilities provided by this service are:

(i) availability monitoring;

(ii) capacity monitoring;

(iii) performance monitoring;

(iv) alert monitoring; and

(v) corrective action upon an event or Incident being highlighted.

(j) Planned unavailability of software shall be performed in such a manner as to minimise the disruption of the AUTHORITY business processing. All periods of planned unavailability shall be agreed with the AUTHORITY and shall not be included in availability calculations within the relevant Service Level.

(k) Planned unavailability shall be performed in accordance with a mutually agreed schedule.

(l) All software and firmware changes and upgrades shall be performed in accordance with Schedule 24 (Change Control).

(m) All software shall be tracked as an Asset in the DSL.

7.2 Hardware Management and Support

(a) The CONTRACTOR shall ensure that all hardware within the scope of its responsibility is appropriately specified for the tasks it performs.

(b) All hardware utilised to provide the Services should be fully supported and maintained.

(c) The CONTRACTOR is required to schedule preventative maintenance in agreement with the AUTHORITY.

(d) All hardware used to provide the Service shall be recorded as an Asset on the Asset Register and tracked accordingly within the CMDB.

8 Service Builds

8.1 The Service Build lifecycle comprises the following stages in the new Service Build lifecycle:

(a) Pre-Sales Stage;

(b) Engagement Stage;

(c) Service Build Stage;

(d) Test Stage; and

(e) Support Stage.

8.2 Pre-Sales Stage

(a) Pre-Sales Stage Process Outputs:

(i) MOU1 document sign-off (if applicable).

(b) The CONTRACTOR shall:

(i) provide input to the AUTHORITY's quarterly forecast plan;

(ii) provide ad-hoc technical support, advice and assistance to the AUTHORITY's Customers, limited to the agreed maximum limit, as described in Schedule 4 (KPIs, Service Levels and Service Credits);

(iii) accept an agreed number of Questionnaire Packs (QPs) per week as defined in Schedule 4 (KPIs, Service Levels and Service Credits) (this number includes any QPs re-submitted);

(iv) schedule an agreed CONTRACTOR resource to attend any pre-sales opportunity as requested.

(c) The AUTHORITY will:

(i) own the pre-sales cycle;

(ii) own the marketing campaigns;

(iii) request the agreed CONTRACTOR resource to attend meetings with the AUTHORITY's Customer, if required, limited to the agreed maximum limit, as described in Schedule 4 (KPIs, Service Levels and Service Credits);

(iv) communicate any lower priority scheduling / re-scheduling dates to the AUTHORITY’s Customer(s) during the course of the Service Build life cycle;

(v) achieve the AUTHORITY’s Customer sign-off of the MOU1 (if applicable);

(vi) provide the first point of contact for the AUTHORITY’s Customers until the QP has been baselined and accepted by all parties;

(vii) make initial contact with the AUTHORITY’s Customer;

(viii) produce and present rolling six monthly forecast plans for the Service Builds to the CONTRACTOR at quarterly planning meetings. This meeting will include a discussion on the potential sales pipeline, timeframes, and project milestones, and their impact on resources;

(ix) present the current work load in progress and following 4 weeks’ planned schedule in detail at the monthly Operations Board meetings;

(x) highlight any requirements for new projects initiated by the AUTHORITY’s Customer at the monthly Operations Board meetings;

(xi) ensure that the AUTHORITY’s Customer will:

(A) contact the AUTHORITY to initiate the Service Build lifecycle;

(B) complete and sign-off MOU1 (if applicable) and deliver it to the AUTHORITY, i.e. to initiate the first stage in the sales cycle.

8.3 Engagement Stage

(a) Engagement Stage Process Outputs:

(i) MOU2 document sign-off (if applicable);

(ii) release QP and the necessary supporting information to assist the AUTHORITY’s Customer to complete the QP to Acceptance Stage;

(iii) the AUTHORITY will raise a Change Request;

(iv) baselined QP accepted by the AUTHORITY, the AUTHORITY’s Customer and the CONTRACTOR

(b) The CONTRACTOR shall:

(i) assign a WP Manager as the named responsible owner to be responsible for the Service Build against the raised Change Request;

(ii) schedule the named WP Manager to attend any engagement meetings as required;

(iii) provide ad-hoc technical support, advice and assistance to the AUTHORITY's Customers, as described in Schedule 4 (KPIs, Service Levels and Service Credits);

(iv) assist the AUTHORITY and the AUTHORITY's Customer to complete the QP;

(v) complete a high level impact assessment on the submitted QP;

(vi) review the proposed deployment dates to Reference and Production Environments;

(vii) provide a draft high level project plan to the AUTHORITY based upon milestones provided by the AUTHORITY's Customers;

(viii) submit the proposed Acceptance Criteria to the AUTHORITY and the AUTHORITY's Customer(s) in relation to the Service Build;

(ix) agree the baselined QP with:

(A) the AUTHORITY's Customer; and

(B) the AUTHORITY;

(x) upon acceptance of the agreed baselined QP by the CONTRACTOR, the CONTRACTOR shall impose full Change Control Procedures to the baselined QP in accordance with Schedule 24 (Change Control);

(xi) confirm appropriate resources are scheduled to meet proposed build, test, and deployment dates as contained within the QP.

(c) The AUTHORITY will:

(i) request CONTRACTOR resource to attend meetings with the AUTHORITY's Customer, if required, as described in Schedule 4 (KPIs, Service Levels and Service Credits);

(ii) provide the first point of contact for the AUTHORITY's Customer(s) until the QP has been baselined and accepted by all parties;

(iii) present the AUTHORITY's Customer with the QP, their responsibilities and deliverables during the Pre-Sales and Engagement Stages;

(iv) schedule a meeting with the AUTHORITY's Customer to discuss the QP and their proposed timeframes and project milestones;

(v) present the AUTHORITY's Customer with sufficient information to enable the AUTHORITY's Customer to complete the review and accept the QP;

(vi) ensure the completion and acceptance of the MOU2 (if applicable) by the AUTHORITY's Customer;

(vii) contact the CONTRACTOR Service Desk during the Pre-Sales or Engagement Stages and log a Service Request to raise a Change Request confirming:

(A) the AUTHORITY’s Customer details; and

(B) any proposed follow-up meeting date requiring the attendance of a WP Manager;

(viii) ensure that the AUTHORITY’s Customer will during the Engagement Stage:

(A) review and agree Acceptance Criteria for the Service Build;

(B) complete the QP with assistance from the AUTHORITY;

(C) complete the baseline QP and present signed-off copy to the AUTHORITY;

(D) deliver against responsibilities assigned in the Reference / Production Acceptance Criteria for both Reference and Production Environments.

(d) The AUTHORITY’s Customer will, during the Engagement Stage:

(i) complete and accept the MOU2 (if applicable) and deliver it to the AUTHORITY;

(ii) provide assistance to the AUTHORITY and/ or the CONTRACTOR to complete the baselined QP; and

(iii) request additional support to complete the QP from the CONTRACTOR, if required, via email to the CONTRACTOR WP Manager.

8.4 Service Build Stage

(a) Service Build Stage Process Outputs:

(i) delivery of Service Build into a Non-Production Environment for the Gateway as defined in the baselined QP;

(ii) detailed project plan agreed by all Parties;

(iii) Acceptance Test Criteria met.

(b) The CONTRACTOR shall:

(i) manage the delivery of Service Build implementation from the receipt of a baselined QP and complete the Service Build and Test Stages successfully to meet scheduled deployment dates into Production and Non-Production Environments;

(ii) apply full Change Control Procedures and management to the baselined QP in accordance with Schedule 24 (Change Control);

(iii) notify the AUTHORITY's Customer of the unique Change Request number for the Service Build, together with the CONTRACTOR Service Desk telephone number to be used when requesting assistance from the CONTRACTOR during the Service Build and Test Stages;

(iv) complete the Service Build and CONTRACTOR Test Stages;

(v) report back to the AUTHORITY and the AUTHORITY's Customer that the Service Build Stage has commenced;

(vi) provide a project plan to the AUTHORITY and the AUTHORITY's Customers based upon milestones provided and which shall be subject to full Change Control Procedures in accordance with Schedule 24 (Change Control);

(vii) track progress against the Service Level and provide regular status updates to the AUTHORITY and the AUTHORITY's Customer;

(viii) release to the AUTHORITY's Customer the test environment, as defined in the baselined QP;

(ix) provide ad-hoc technical support, advice and assistance to the AUTHORITY's Customer(s), as described in Schedule 4 (KPIs, Service Levels and Service Credits) including;

(A) technical support, advice and assistance to AUTHORITY's Customer(s) for the installation and support of PKCS#10 certificates and Gateway tokens;

(x) ensure Gateway secure letters and emails are received by the AUTHORITY's Customer;

(xi) ensure a testing strategy is available for Service Builds, including

(A) a standardised test plan for the AUTHORITY's Customer; and

(B) acceptance criteria for each Gateway Environment;

(xii) produce a test assessment (system test result);

(xiii) produce a release sign-off for the test environment, as defined in the baselined QP;

(xiv) receive the reference booking form from the AUTHORITY's Customer;

(xv) provide Gateway IP addresses (Helpdesk, Reference, etc.) to the AUTHORITY's Customers.

(xvi) create Helpdesk accounts for the AUTHORITY's Customers;

(xvii) ensure that the AUTHORITY’s Customers will:

(A) complete successful testing in the defined environments as stipulated in the agreed Gateway Acceptance criteria;

(B) raise a Service ticket to track any defects or issues experienced during Test Stage;

(C) resolve any outstanding application or connectivity issues;

(D) complete all Reference Acceptance Criteria;

(E) provide a regular status update to the CONTRACTOR WP Manager;

(F) procure and install, DIS box (if applicable);

(G) submit test plans to the CONTRACTOR for review;

(H) ensure connectivity between the Gateway and the AUTHORITY’s Customer(s);

(I) send the reference booking form to the CONTRACTOR.

8.5 Test Stage

(a) Test Stage Process Outputs:

(i) delivery of Service Build, as defined in the baselined QP;

(ii) AUTHORITY’s Customer UAT sign-off;

(iii) Operational Acceptance Test (OAT) sign-off;

(iv) Production Acceptance Criteria met.

(b) The CONTRACTOR shall:

(i) authorise Service Build deployment to Reference once all the Reference Acceptance Criteria have been met;

(ii) authorise the deployment of the Service Build to the Gateway Environments as defined in the baselined QP;

(iii) update the AUTHORITY and the AUTHORITY’s Customer that the Service Build is ready and available for UAT testing on the Gateway Environment as defined in the baselined QP;

(iv) provide ad-hoc technical support, advice and assistance to the AUTHORITY’s Customers, as described in Schedule 4 (KPIs and Service Levels);

(v) ensure connectivity between the Gateway and the AUTHORITY’s Customer(s);

(vi) provide Gateway Helpdesk application training and a Helpdesk User Guide to the AUTHORITY’s Customers as defined in the agreed project plan;

(vii) ensure that test Gateway Mail is produced and approved;

(viii) produce a release sign-off for Production, confirming UAT & OAT have been passed;

(ix) Payment Service and Alert Service activated (as applicable);

(x) ensure that the AUTHORITY’s Customer has checked that business responses (message class) have been sent back to the Gateway;

(xi) ensure that the AUTHORITY’s Customer will during the Test Stage:

(A) complete successful UAT using the Reference Environment;

(B) raise an Incident ticket to track any issues experienced during testing on Reference;

(C) contact the CONTRACTOR via the CONTRACTOR Service Desk to confirm successful completion of UAT and UAT sign-off;

(D) complete all their responsibilities listed on the Production Acceptance Criteria checklist;

(E) confirm the Gateway User Interface links and text is accurate on the Reference Environment;

(F) provide the DIS box (if applicable) for the Production Environment;

(G) provide test exit reports to the CONTRACTOR for review;

(H) ensure that the Production certificate(s) are successfully installed;

(I) ensure that the automatic Known Facts loading is tested successfully;

(J) approve test Gateway Mail;

(K) deliver against responsibilities assigned in the Reference Acceptance Criteria for Reference deployment.

8.6 Support Stage

(a) For the avoidance of doubt, the Support Stage is performed throughout the whole Service Build lifecycle.

(b) The CONTRACTOR shall:

(i) accept the deployments as defined in the baselined QP;

(ii) action the Service Build deployment, including the loading of any branding pages (if applicable) as defined in the baselined QP;

(iii) deploy the Release as defined in the baselined QP;

(iv) produce a Post Implementation Review (PIR) for review by the AUTHORITY and the AUTHORITY's Customer after deployment of the Service Build to Production in accordance with Schedule 4 (KPIs and Service Levels);

(v) deliver against responsibilities assigned in the Production Acceptance Criteria for Production deployment;

(vi) provide the AUTHORITY with a plan scheduling all Service Build deployments;

(vii) provide as part of the support process required to underpin the delivery of the AUTHORITY's Customer Service Builds:

(A) manual clearing of Gateway queues i.e. suspend queue;

(B) update of Gateway pages;

(C) ad-hoc tracing (investigation) of Gateway Environments;

(D) maintain and update Gateway Portal Pack;

(viii) provide input to trends analysis at the Strategy and Planning Board in accordance with Schedule 13 (Governance and Reporting);

(ix) produce and maintain Gateway technical and business facing documentation;

(x) provide review of business and technical documentation produced by the AUTHORITY's Customers;

(xi) provide review of business and technical documentation produced by the AUTHORITY, the AUTHORITY's Customers and their suppliers;

(xii) produce a communications strategy (internal and external) for all Service Builds;

(xiii) provide knowledge / skills sessions to AUTHORITY when required.

(xiv) track progress against the project plan and provide feedback to the AUTHORITY and the AUTHORITY's Customers;

(xv) define, document and manage Acceptance Criteria;

(xvi) ensure that a Support Stage review is held.

(c) The AUTHORITY will:

(i) provide feedback to the CONTRACTOR by exception highlighting any changes to the agreed short term monthly outlook of new deployments;

(ii) own the customer relationship management with the AUTHORITY's Customer(s);

(iii) attend PIR meeting.

9 Application Development Service

9.1 The specific Application Development Services are as described in Schedule 22 (Development Services).

10 Other Services

10.1 Technical Support Services

(a) The CONTRACTOR shall manage the Gateway hardware maintenance contracts pertaining to all hardware with the exception of network hardware which is covered within paragraph 10.2 (a).

(b) The CONTRACTOR shall assist the AUTHORITY with the renewal of these contracts.

(c) The CONTRACTOR shall maintain a record of all active and completed work instructions.

10.2 Network Services

(a) The CONTRACTOR shall manage the network hardware support contract on behalf of the AUTHORITY.

(b) The CONTRACTOR shall assist the AUTHORITY in the renewal of the network hardware maintenance contract.

11 Resourcing

11.1 The CONTRACTOR shall implement resource management processes to ensure effective:

(a) succession planning;

(b) knowledge transfer;

(c) appropriate security clearance;

(d) availability of, retention of and future planning of required skills; and

(e) staff induction and training.

11.2 The CONTRACTOR shall maintain a database of all CONTRACTOR Personnel and roles containing

(a) a profile of skills;

(b) competencies; and

(c) experience.

11.3 The CONTRACTOR shall ensure that all CONTRACTOR Personnel meet the skills and competencies required for the roles in which they are deployed, or planned to be deployed to deliver the Gateway and the Services.

11.4 The CONTRACTOR shall use this database to escalate to the AUTHORITY where the profile of skills for CONTRACTOR Personnel at any given time does not meet all of documented skills and competencies for each of the roles on the account.

11.5 The CONTRACTOR shall maintain details of CONTRACTOR Personnel who have previously worked on the Gateway to facilitate swift resource fulfilment.

11.6 The resources provided by the CONTRACTOR to deliver application support and maintenance shall cover all skills required to fulfil fault resolution and application testing obligations.

11.7 The CONTRACTOR shall use Best Practices in resource management, including:

(a) career paths and progression including:

(i) succession planning;

(ii) training; and

(iii) internal promotions;

(b) clearly defined responsibilities and empowerment;

(c) positive and frequent communication.

12 Core Committed Team

12.1 The CONTRACTOR shall provide a Core Committed Team comprising the core design skills and knowledge of the Gateway products in the following areas:

(a) Gateway applications and tools;

(b) underlying COTS packages supporting the Gateway;

(c) Gateway testing and any automated frameworks; and

(d) Gateway development and Release processes.

12.2 The Core Committed Team shall:

(a) support the AUTHORITY's business development activities with the AUTHORITY's Customer(s);

(b) provide technical advice and guidance to the AUTHORITY on Gateway design and development;

(c) participate in the CONTRACTOR's Continuous Improvement Programme activities, in accordance with Schedule 6 (Continuous Improvement Programme);

(d) set and maintain the testing requirements for Gateway Releases; and

(e) work closely with the AUTHORITY and other CONTRACTOR teams to promote the evolution and technical development of the Gateway applications and its associated operating environments.

13 Ad-Hoc Projects Service

13.1 To the extent that the AUTHORITY requires any services falling outside the scope of the either the Services described in this Schedule 2 (Services) or Development Services as defined in Schedule 22 (Development Services) the AUTHORITY may request the CONTRACTOR to provide additional Ad-Hoc Project Services.

13.2 Any such Ad-Hoc Project Service requests shall be made to the CONTRACTOR's Service Desk in accordance with Schedule 2 (Services).

13.3 The CONTRACTOR shall provide support to the AUTHORITY's Customers which may require to test the Gateway during weekend periods at an additional charge in accordance with Schedule 15 (Charges).

(a) The AUTHORITY will confirm in writing to the CONTRACTOR's Service Desk the specific requirements for coverage and the scope of testing to be performed ten (10) Working Days in advance of the required date.

(b) The CONTRACTOR shall provide the AUTHORITY with the requisite charge within one (1) Working Day of receipt of the request.

(c) The AUTHORITY will confirm acceptance of the charge within one (1) Working Day of receipt.

(d) In the event that the AUTHORITY can not comply with paragraph 13.3 (a), the CONTRACTOR shall use reasonable endeavours to comply with the request which shall be charged in accordance with Schedule 15 (Charges).

13.4 The CONTRACTOR shall:

(a) ensure that the Gateway is accredited and measured in line with the Payment Card Industry Data Security Standard (PCI DSS);

(b) mutually agree with the AUTHORITY the required accreditation and measurement activities; and

(c) raise appropriate Change Requests in relation to technical changes, enhancements, associated project effort and resources should any amendments be required to the Gateway to maintain compliance.