## 5.8 Access Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 5.8.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Access Management Policies and Processes. |
| 5.8.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Access Management Policies and Processes in the delivery of the Services |
| 5.8.3 | L3 | Supplier | The Supplier shall work with the Service Desk Supplier and the Authority to implement the Authority's Access Management Policies and Processes which will provide a standard way of enabling access to the Services. |
| 5.8.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Access Management that are aligned to the Authority's Access Management Policies and Processes and shall submit them to the Authority for approval. |
| 5.8.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Access Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 5.8.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Access Management and report such non-compliance to the Authority. |
| 5.8.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Access Management, the Supplier shall bring this to the Authority's attention. |
| 5.8.8 | L3 | Supplier | The Supplier shall allow the Authority and the Authority's Security Operations Centre (SOC) Supplier access to audit trails and logs as agreed and documented in the Authority's Information Security Policy and Standards. |
| 5.8.9 | L3 | Supplier | The Supplier shall verify that all access requests are approved in accordance with the Authority's Access Management Policies and Processes. |
| 5.8.10 | L3 | Supplier | The Supplier shall, in relation to the Services, add, amend or remove access to data, systems, databases, and applications on receipt of an approved access request. |
| 5.8.11 | L3 | Supplier | The Supplier shall be responsible for password management, where in scope, which includes:<br>a. performing authorised End User password resets in accordance with the Authority's Information Security Policy and Standards;<br>b. coordinating authorised End User password changes and changing local End User identifications and passwords as required and ensuring password Policy is enforced; and<br>c. encrypting passwords according to the Authority's Information Security Management Policies and Processes. |
| 5.8.12 | L3 | Supplier | The Supplier shall be responsible for elevated rights management, within the scope of their Services, as set out in the Authority's Information Security Policy and Standards, which includes:<br>a. maintaining defined access controls for protection of system software and the Authority's environment resources (for example, the system control program, its access control mechanisms), and reviewing and updating periodically, according to the Authority's Access Management Policies and Processes;<br>b. ensuring that privileged account End Users are only provided access necessary to perform duties assigned and that Authorised End Users are not provided systems administrator access unless an exception is granted in accordance with the Authority's Access Management Policies and Processes; |

| | | | |
|---|---|---|---|
| | | | c. providing designated Supplier Personnel, Authority Personnel, and Other Supplier personnel with supervisor-equivalent End User identifications and passwords where reasonably required to provide the Services in accordance with the Authority's Access Management Policies and Processes;<br>d. managing critical passwords across all platforms for emergency and operational purposes, such as elevating privileges, root passwords, and service account passwords; and<br>e. ensuring that privileged account End Users are only provided access necessary to perform duties assigned and that Authorised End Users are not provided systems administrator access unless an exception is granted in accordance with the Authority's Access Management Policies and Processes. |
| 5.8.13 | L3 | Supplier | The Supplier shall monitor End Users of the systems and services for authorised access, and monitor, review, and respond in a timely and appropriate manner to access violations and report findings on a monthly basis in accordance with the Authority's Information Security Policies and Standards. |
| 5.8.14 | L3 | Supplier | The Supplier shall run monthly reports to identify those accounts that should be removed on Supplier-operated systems and remove them following approval from the Authority. |
| 5.8.15 | L3 | Supplier | The Supplier shall recertify their own resource and all relevant Authority End Users in accordance with the Authority's Information Security Management Policies and Processes and in line with Schedule 2.4 (*Security Management*). |
| 5.8.16 | L3 | Supplier | The Supplier shall notify immediately the Authority in the event that the Supplier becomes aware of a security violation or unauthorised attempt to access or alter the Authority Data, where the notification and escalation is made according to the Authority's Information Security Policy and Standards. |
| 5.8.17 | L3 | Supplier | The Supplier shall provide the Authority with follow-up reports on all violation and access attempts within 24 hours from such attempt being discovered by the Supplier, and shall retain documentation of the investigation in accordance with the provisions of this Agreement, including Schedule 7.5 (*Reports and Audit Rights*). |
| 5.8.18 | L3 | Supplier | The Supplier shall capture data regarding routine access and exceptions for audit trail purposes and make such data available to the Authority upon request. |
| 5.8.19 | L3 | Supplier | The Supplier shall immediately upon the request of the Authority, remove or restrict the End User, or particular group of End Users, access rights to the services and systems. |
| 5.8.20 | L3 | Supplier | The Supplier shall operate a joiner, mover, leaver (JML) Process on all Supplier Personnel connected with the provision of Services and ensure that access privileges are suspended on notification of a leaver. |
| 5.8.21 | L3 | Supplier | The Supplier shall work with the Authority to design, implement and enforce a Role Based Access Control (RBAC) across its Services. |
| 5.8.22 | L3 | Supplier | The Supplier shall, in relation to the Services, manage Directory Services and group policy objects on domains to support the Authority environment and enable Other Suppliers to manage group policy objects as required, and in agreement with the Authority, through delegated rights. |
| 5.8.23 | L3 | Supplier | The Supplier shall:<br>a. add, change and delete groups as per access requests;<br>b. assign End Users to groups as per access requests; and<br>c. remove End Users out of groups as per access request. |
| 5.8.24 | L3 | Supplier | The Supplier shall create, maintain and delete Access Profiles, as requested by the Authority. |
| 5.8.25 | L3 | Supplier | The Supplier shall inform the Authority if an access request exceeds, or is expected to exceed, target Resolution Time. |

| | | | |
|---|---|---|---|
| 5.8.26 | L3 | Supplier | The Supplier shall escalate issues to the appropriate levels for resolution in accordance with escalation Procedures approved by the Authority and detailed in the Access Management Policies and Processes. |
| 5.8.27 | L3 | Supplier | The Supplier shall identify and escalate requests for access to systems and data to which the End User is not allowed access ("toxic" access requests) to ensure appropriate access is maintained. An example could be where an End User has requested the ability to raise and approve purchase orders. |
| 5.8.28 | L3 | Supplier | The Supplier shall close an access request in accordance with the closure Procedure defined in the Authority's Access Management Policies and Processes. |

# 6. Monitor and Manage

## 6.1 Availability Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 6.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Availability Management Policies and Processes. |
| 6.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Availability Management Policies and Processes in the delivery of their Services. |
| 6.1.3 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Availability Management that are aligned to the Authority's Availability Management Policies and Processes and shall submit them to the Authority for approval. |
| 6.1.4 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Availability Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 6.1.5 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Availability Management and report such non-compliance to the Authority. |
| 6.1.6 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Availability Management, the Supplier shall bring this to the Authority's attention. |
| 6.1.7 | L3 | Supplier | The Supplier shall work with the IT Operations Centre Supplier and the Authority to implement the Authority's Availability Management Policies and Processes. |
| 6.1.8 | L3 | Supplier | The Supplier shall work with the Authority to understand the Authority's availability requirements. |
| 6.1.9 | L3 | Supplier | The Supplier shall have the appropriate monitoring and measurement in place to support and measure against the Authority's requirements for Availability, as defined in the Authority's Availability Management Policies and Processes and Performance Indicators. |
| 6.1.10 | L3 | Supplier | The Supplier shall gather Service Availability and component availability data for the elements of the Supplier's Services and record and maintain this data. |
| 6.1.11 | L3 | Supplier | The Supplier shall analyse, manage and report on all key elements of Availability in accordance with the Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*). Such analysis shall include availability, reliability, maintainability and serviceability measures. |
| 6.1.12 | L3 | Supplier | The Supplier shall produce availability and reliability trend analysis as required by the Authority. |
| 6.1.13 | L3 | Supplier | The Supplier shall design the Services ensuring the required levels of Availability, reliability, maintainability, serviceability, security and Performance Indicators are met. |
| 6.1.14 | L3 | Supplier | The Supplier shall conduct proactive management and risk analyses to test and analyse predicted availability of the Services. |
| 6.1.15 | L3 | Supplier | The Supplier shall identify, select and implement any agreed countermeasures, justified by the identified risks in terms of their potential impact on the Services, if Service Availability failure occurs. |
| 6.1.16 | L3 | Supplier | The Supplier shall establish, maintain and implement a planned and preventive maintenance strategy, in relation to Availability, to be agreed with the Authority. |

| | | | |
|---|---|---|---|
| 6.1.17 | L3 | Supplier | The Supplier shall review all Operational Change Requests in respect of the Services, for impact on Availability and ensure that the proposed Change meets reliability, maintainability and serviceability requirements, and the relevant Performance Indicators. |
| 6.1.18 | L3 | Supplier | The Supplier shall investigate every instance of below target availability. |
| 6.1.19 | L3 | Supplier | The Supplier shall, in relation to the Services, provide early warning of potential or actual availability issues. |
| 6.1.20 | L3 | Supplier | The Supplier shall proactively identify components that are susceptible to Service Availability failure and recommend cost-effective solutions for consideration and approval. |
| 6.1.21 | L3 | Supplier | The Supplier shall review performance against the Availability Plan developed and agreed with the Authority and recommend remedial actions to the Authority. |
| 6.1.22 | L3 | Supplier | The Supplier shall make available to the Authority, real-time information on Service Availability via the Service Portal and a drill down view for the Authority Service Management function. |

## 6.2 Event Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 6.2.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Event Management Policies and Processes. |
| 6.2.2 | L3 | Supplier | The Supplier shall at all times adhere to the Authority's Event Management Policies and Processes in the delivery of the Services. |
| 6.2.3 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Event Management that are aligned to the Authority's Event Management Policies and Processes and shall submit them to the Authority for approval. |
| 6.2.4 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Event Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 6.2.5 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Event Management and report any non-compliance to the Authority. |
| 6.2.6 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Event Management, the Supplier shall bring this to the Authority's attention. |
| 6.2.7 | L3 | Supplier | The Supplier shall work with the IT Operations Centre Supplier, and the Authority, to implement the Authority's Event Management Policies and Processes |
| 6.2.8 | L3 | Supplier | The Supplier shall provide Event Management monitoring, tracking and reporting in relation to the Services and where agreed with the Authority. |
| 6.2.9 | L3 | Supplier | The Supplier shall, establish and maintain a proactive and automated Event Management Process to ensure all appropriate Services are monitored and that appropriate Events are identified, promptly actioned, recorded and reported. |
| 6.2.10 | L3 | Supplier | The Supplier's Event Management Process and automated tools shall include:<br>a. accurately providing data such that measuring Supplier's performance against Performance Indicators is achievable;<br>b. providing functionality to set thresholds for tuning to improve performance and utilisation; |

| | | | |
|---|---|---|---|
| | | | c. automatically triggers response options (e.g. Incident record generation, scripts); and<br>d. providing a set of Event detection, diagnostic, and tracking software and equipment to enable the automation of monitoring, detection, and resolution of Events associated with the cross functional services as documented in the Event Management Policies and Processes. |
| 6.2.11 | L3 | Supplier | The Supplier shall ensure that appropriate Event notifications are configured on all agreed components and captured within the Event monitoring tools. |
| 6.2.12 | L3 | Supplier | The Supplier shall perform monitoring activities, including:<br>a. systems processing;<br>b. monitoring, where appropriate, the environment, alarm systems and environmental controls; and<br>c. monitoring IT Systems, Infrastructure and, where agreed, application services in accordance with the Authority's Event Management Policies and Processes. |
| 6.2.13 | L3 | Supplier | The Supplier shall integrate its own and third party Events and Alerts with the ITSM Product for the purpose of Event correlation and aggregation. |
| 6.2.14 | L3 | Supplier | The Supplier shall set Event thresholds agreed with and approved by the Authority, which may be subject to change during the Term. |
| 6.2.15 | L3 | Supplier | The Supplier shall implement Event thresholds in cooperation with Other Suppliers, and as approved by the Authority. |
| 6.2.16 | L3 | Supplier | The Supplier shall provide proactive (in addition to reactive) monitoring and management in order to enhance the stability and function of the cross functional environment. |
| 6.2.17 | L3 | Supplier | The Supplier shall define Event correlation, categorisation and closure rules and implement them. Upon detection of an Event, the Supplier shall filter by classification and trigger the appropriate action. |
| 6.2.18 | L3 | Supplier | The Supplier shall, establish and maintain Event escalation Procedures in accordance with the Authority's Event Management Policies and Processes. |
| 6.2.19 | L3 | Supplier | The Supplier shall provide Event trend analysis, in accordance with the Authority's Event Management Policies and Processes. |
| 6.2.20 | L3 | Supplier | The Supplier shall ensure that Events and Incidents are regularly identified and reviewed to improve Event monitoring capabilities. |
| 6.2.21 | L3 | Supplier | The Supplier shall, upon detection of an Event, filter by classification (such as informative, alert required, exception, and so forth) and trigger the appropriate action. |
| 6.2.22 | L3 | Supplier | The Supplier shall receive, and handle Events generated from other sources, as agreed by the Supplier and the Other Suppliers. For each Event, a documented action must be defined between the Supplier and the Other Suppliers. |
| 6.2.23 | L3 | Supplier | The Supplier shall categorise Events (e.g. informal, warning, exception) based on defined categorisation rules in accordance with the Authority's Event Management Policies and Processes. |
| 6.2.24 | L3 | Supplier | The Supplier shall ensure that the correct priority level is attached to each Event and is available to the Authority for further processing. |
| 6.2.25 | L3 | Supplier | The Supplier shall correlate Events and initiate the appropriate response. |
| 6.2.26 | L3 | Supplier | The Supplier shall correlate Events to facilitate Problem Management and root cause analysis of Service failures. |
| 6.2.27 | L3 | Supplier | The Supplier shall participate in joint coordination meetings organised by the Authority or the Authority's IT Operations Centre Supplier to determine response selection for cross-functional Events. |
| 6.2.28 | L3 | Supplier | The Supplier shall make Event-related root cause analysis and trend analyses available to the Authority. |

| | | | |
|---|---|---|---|
| 6.2.29 | L3 | Supplier | The Supplier shall prevent unnecessary rerouting and/or reassignments of Events in accordance with the Authority's Event Management Policies and Processes. |
| 6.2.30 | L3 | Supplier | The Supplier shall support the Authority in the maintenance and updating of the operational documentation for all operations Procedures and Services based on Event trending information including:<br>a. Authority's Service Management Policies and Processes; and<br>b. revised business Procedures. |
| 6.2.31 | L3 | Supplier | The Supplier shall participate in joint coordination meetings organised by the Authority to determine response selection for cross-functional Events. |

## 6.3 Major Incident Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 6.3.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Major Incident Management Policies and Processes. |
| 6.3.2 | L3 | Supplier | The Supplier shall at all times adhere to the Authority's Major Incident Management Policies and Processes in the delivery of the Services. |
| 6.3.3 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Major Incident Management that are aligned to the Authority's Major Incident Management Policies and Processes and shall submit them to the Authority for approval. |
| 6.3.4 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Major Incident Management, including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 6.3.5 | L3 | Supplier | The Supplier shall monitor the compliance of and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Major Incident Management and report any non-compliance to the Authority. |
| 6.3.6 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Major Incident Management, the Supplier shall bring this to the Authority's attention. |
| 6.3.7 | L3 | Supplier | The Supplier shall work with the IT Operations Centre Supplier, the Authority and Other Suppliers to implement the Authority's Major Incident Management Policies and Processes which will provide a standard way of managing common types of Major Incidents. |
| 6.3.8 | L3 | Supplier | The Supplier shall process each Major Incident in accordance with the Severity level allocated by the IT Operations Centre Supplier and the Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*). |
| 6.3.9 | L3 | Supplier | The Supplier shall keep Service Tickets updated in accordance with the Major Incident Management Policies and Processes. |
| 6.3.10 | L3 | Supplier | The Supplier shall notify the Authority of anticipated Resolution Times for Major Incidents, in line with the Authority's Policies and Processes. |
| 6.3.11 | L3 | Supplier | The Supplier shall perform investigative and diagnostic activities to identify workarounds for each Major Incident. |
| 6.3.12 | L3 | Supplier | The Supplier shall inform the Authority of Major Incidents that are expected to exceed target Resolution Times. |
| 6.3.13 | L3 | Supplier | The Supplier shall provide prompt notification to the IT Operations Centre Supplier of system outages. |
| 6.3.14 | L3 | Supplier | The Supplier shall, where the Event Management has detected a Major Incident, identify and capture information about the nature of the failure. |

| | | | |
|---|---|---|---|
| 6.3.15 | L3 | Supplier | The Supplier shall cooperate with the Authority on any escalations. |
| 6.3.16 | L3 | Supplier | The Supplier shall inform the Authority if Major Incidents exceed or are expected to exceed their target Resolution Times. |
| 6.3.17 | L3 | Supplier | The Supplier shall escalate issues to the appropriate levels for resolution in accordance with escalation Procedures. |
| 6.3.18 | L3 | Supplier | As directed by the Authority, the Supplier shall attend meetings with the Authority and the Other Suppliers, to support cross functional activities and collaborate as required to diagnose escalated Major Incidents. |
| 6.3.19 | L3 | Supplier | The Supplier shall support the Authority and the Other Suppliers in the diagnosis of a Major Incident, the definition of resolution options and the identification of the Service Suppliers that need to conduct further investigation or resolution activities. |
| 6.3.20 | L3 | Supplier | The Supplier shall resolve Major Incidents. |
| 6.3.21 | L3 | Supplier | The Supplier shall ensure that for each assigned Major Incident, Services are restored as promptly and in all cases within the Resolution Times applicable to the Incident Severity and relevant Performance Indicators and act proactively and collaborate with all other parties (including Other Suppliers) as needed in order to resolve Incidents. |
| 6.3.22 | L3 | Supplier | The Supplier shall participate, with Other Suppliers, in 'all hands' meetings organised by the Authority or the Service Desk Supplier on the Authority's behalf. |
| 6.3.23 | L3 | Supplier | The Supplier shall provide resolution plans for Severity 1 and Severity 2 Incidents and seek approval of the Authority where such resolution impacts other Services. |
| 6.3.24 | L3 | Supplier | Where Incidents relate to assets, the Supplier shall, where appropriate, provide update details for the CMDB, or coordinate through the relevant agreed Process to confirm when updates are made. |
| 6.3.25 | L3 | Supplier | Where Incidents relate to the changing of software or hardware assets, the Supplier shall, where appropriate, provide update details for the CMDB or coordinate with the relevant agreed Process to confirm updates are made. The Supplier shall, if a Change to the Services is required to implement resolution or workaround, submit an Operational Change Request in accordance with the Authority's Change Management Policies and Processes or seek exemption from the Change Management Policies and Processes from the Authority as appropriate. |
| 6.3.26 | L3 | Supplier | The Supplier shall, if required, generate a Problem Record from a Major Incident. |
| 6.3.27 | L3 | Supplier | If new workarounds or resolutions are applied, the Supplier shall coordinate with the Authority to open a Problem Record and log a new Problem, workaround and known error as appropriate. |
| 6.3.28 | L3 | Supplier | The Supplier shall conduct necessary Tests to ensure that a Major Incident is resolved. |
| 6.3.29 | L3 | Supplier | The Supplier shall, if a Change to the Services is required to implement the resolution or a workaround, submit an Operational Change Request in line with the Authority's Change Management Policies and Processes. |
| 6.3.30 | L3 | Supplier | The Supplier shall for Major Incidents take remedial action to ensure that the Incident does not re-occur and follow-up to ensure that the remedial action has been taken within reasonable timescales. |

# 7. Control

## 7.1 Introduction

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Change Management Policies and Processes. |
| 7.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Change Management Policies and Processes in the delivery of their Services. |
| 7.1.3 | L3 | Supplier | The Supplier shall work with the Service Desk Supplier, the IT Operations Centre Supplier, the Authority and Other Suppliers on the implementation of the Authority's Change Management Policies and Processes. |
| 7.1.4 | L3 | Supplier | The Supplier shall perform an evaluation of both intended and unintended effects of the proposed Change, or cross functional Changes, if it affects its Services. |
| 7.1.5 | L3 | Supplier | The Supplier shall provide an Impact Assessment in relation to proposed Changes that could affect the delivery of its Services in accordance with the provisions of Schedule 8.2 (*Change Control Procedure*). |
| 7.1.6 | L3 | Supplier | The Supplier shall evaluate the predicted performance of the Operational Change including:<br>a. End User requirements (including Acceptance Criteria); and<br>b. evaluating the predicted performance, and/or the outcome of the predicted performance, versus the Acceptance Criteria. |
| 7.1.7 | L3 | Supplier | The Supplier shall, after implementation of a Change, provide input regarding actual performance of the Service versus the Acceptance Criteria. |
| 7.1.8 | L3 | Supplier | The Supplier shall perform a Supplier specific risk assessment, if required by the Authority, for cross functional Changes, based on the required specifications, predicted performance and the Acceptance Criteria for the proposed Change and report evaluation findings to and await further direction subject to the Authority's Change Management Policies and Processes |

## 7.2 Change Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.2.1 | L3 | Supplier | The Supplier shall, in line with Authority's Change Management Policies and Processes, collaborate in the operation of the Authority's Change Advisory Board (CAB) by providing input, including:<br>a. evaluations of Change impact;<br>b. recommendations for approval or otherwise;<br>c. recommending an implementation plan; and<br>d. recommending appropriate participation. |
| 7.2.2 | L3 | Supplier | The Supplier shall receive, review and approve Changes according to the Change authorisation matrices defined in the Authority's Change Management Policies and Processes |
| 7.2.3 | L3 | Supplier | The Supplier shall retain overall responsibility for all Operational Changes allocated to them until the Operational Change is closed, subject to the Authority's CAB approval. |

| | | | |
|---|---|---|---|
| 7.2.4 | L3 | Supplier | The Supplier shall ensure requirements for new Services shall be handled through the Authority's Change Management Policies and Processes, and the Supplier shall work with the Authority and the Other Suppliers to assess the impact of these requirements on the Authority's Operating Environment. |
| 7.2.5 | L3 | Supplier | The Supplier shall provide, as directed by the Authority, necessary information from the time an Operational Change is recorded through to the closure, also providing any follow-up communications and report work required post-resolution to the Authority and to Other Suppliers. |
| 7.2.6 | L3 | Supplier | The Supplier shall update all operational and other documentation affected by the Operational Change. |
| 7.2.7 | L3 | Supplier | The Supplier shall manage the effective entry of Operational Change Records into the ITSM Product, including, the correlation of associated Incidents, Problems and Known Errors. |
| 7.2.8 | L3 | Supplier | The Supplier shall create an Operational Change Record detailing the lifecycle for every Operational Change Request submitted (even those that are failed or subsequently rejected) and shall store the Operational Change Records in the ITSM Product. |
| 7.2.9 | L3 | Supplier | The Supplier shall identify the Operational Change category and the information set out in the CMDB and associate the Operational Change Record to the relevant Configuration Items. |
| 7.2.10 | L3 | Supplier | The Supplier will ensure that prior to the authorisation of Operational Changes, the requests for Operational Change contain information including, but not limited to:<br>a. verified Implementation Plans;<br>b. post Implementation review;<br>c. Acceptance Criteria;<br>d. back out plans or remediation plans; and<br>e. plans for handover to operational support |
| 7.2.11 | L3 | Supplier | The Supplier shall, where required, cooperate with the Authority and the Other Suppliers and designated representatives to minimise disruption of normal business processes and proper receipt of the Services, including:<br>a. carrying out activities required to deliver the Operational Change, such as making changes to individual components and coordinating Operational Changes across all components within its remit;<br>b. controlling systems and activities required by moves, upgrades, replacements, migrations, and so forth;<br>c. Testing and roll-back plans for every Operational Change Request; and<br>d. providing information to the Authority in accordance with the Authority's Change Management Policies and Processes on the outcome of any Operational Change and the updated status after each Operational Change is implemented. |
| 7.2.12 | L3 | Supplier | The Supplier shall monitor and report on the Operational Change implementation. |
| 7.2.13 | L3 | Supplier | The Supplier shall, if there is a need for Emergency Change(s), provide the Authority with as much notice as reasonably practical and perform such maintenance, in agreement with the Authority, to minimise interference with the business and operational needs of the Authority. |
| 7.2.14 | L3 | Supplier | The Supplier shall fully Test Operational Changes and resolve faults, if possible, prior to production start-up, including, where possible, inter-operability Testing and report Test results back to the Authority. |
| 7.2.15 | L3 | Supplier | The Supplier shall update all operational and other documentation affected by the Operational Change. |
| 7.2.16 | L3 | Supplier | The Supplier shall escalate issues to the appropriate levels for resolution in accordance with escalation Procedures approved by the Authority. |

| | | | |
|---|---|---|---|
| 7.2.17 | L3 | Supplier | The Supplier shall support post implementation reviews of Operational Changes to identify opportunities for improvement. |
| 7.2.18 | L3 | Supplier | The Supplier shall manage, conduct and support joint reviews of any subsequent Operational Change failure so that the root causes of post-Operational Change issues can be identified and, where appropriate, linked to the originating Operational Change activity. In addition, the Supplier shall implement any improvements required to prevent a recurrence. |
| 7.2.19 | L3 | Supplier | The Supplier shall close and update the Operational Change Record with all the details of the Operational Change in accordance with the Authority's Change Management Policies and Processes, including linking any Incidents caused by the Operational Change or implementation thereof. |
| 7.2.20 | L3 | Supplier | The Supplier shall link failed Operational Changes to resultant Incident Records in the ITSM Product. |
| 7.2.21 | L4 | Authority | The Authority shall provide a list of Authorised End Users able to approve Emergency Changes. |
| 7.2.22 | L3 | Supplier | Where an Emergency Change is required, the Supplier shall obtain Emergency Change approval and follow the Emergency Change Process as described in the Authority's Change Management Policies and Processes |

## 7.3 Service Asset and Configuration Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.3.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Asset and Configuration Management Policies and Processes. |
| 7.3.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Service Asset and Configuration Management Policies and Processes in the delivery of the Services. |
| 7.3.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Service Asset and Configuration Management Policies and Processes. |
| 7.3.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Service Asset and Configuration Management that are aligned to the Authority's Service Asset and Configuration Management Policies and Processes and shall submit them to the Authority for approval. |
| 7.3.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Service Asset and Configuration Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 7.3.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Service Asset and Configuration Management and report such non-compliance to the Authority. |
| 7.3.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Service Asset and Configuration Management, the Supplier shall bring this to the Authority's attention. |
| 7.3.8 | L3 | Supplier | The Supplier shall manage the configuration of SaaS services as agreed with the Authority, in line with the agreed configuration documents. |
| 7.3.9 | L3 | Supplier | The Supplier shall provide the individual data elements for each asset so that its attributes can be determined, such as ownership (including leased equipment), asset type, model and release number, Site location, country, any physical address, compliance with standards and system priority, applications, contact details, and criticality rating etc., as required by its own service management functions. |

| | | | |
|---|---|---|---|
| 7.3.10 | L3 | Supplier | The Supplier shall ensure that only authorised and identifiable Configuration Items, including for example operations documents, equipment, software and applications, are accepted and are recorded from receipt to disposal. |
| 7.3.11 | L3 | Supplier | The Supplier shall ensure it initiates and oversees auto discovery and other methods of reconciliation in order to verify the accuracy of the asset inventory. |
| 7.3.12 | L3 | Supplier | The Supplier shall ensure they use applicable asset auto-discovery tools. |
| 7.3.13 | L3 | Supplier | The Supplier shall ensure that Configuration Items are uniquely identified and defined by attributes that describe their functional and physical characteristics as defined by the Authority. |
| 7.3.14 | L3 | Supplier | The Supplier shall enable discovery access to their estate for the purposes of CMDB population. |
| 7.3.15 | L3 | Supplier | The Supplier shall provide the individual data elements for each asset as required. |
| 7.3.16 | L3 | Supplier | The Supplier shall provide necessary information for reporting of service configuration and asset items to the Authority. |
| 7.3.17 | L3 | Supplier | The Supplier shall ensure that Configuration Items are recorded from receipt to disposal. The method of update will be agreed with the Authority. |
| 7.3.18 | L3 | Supplier | The Supplier shall ensure that Configuration Items (CIs) are identified in the CMDB by attributes that describe their functional and physical characteristics as defined by the Authority. |
| 7.3.19 | L3 | Supplier | The Supplier shall maintain accurate configuration data for the Configuration Items, including for example operations documents, equipment, software and applications used to provide the Services. |
| 7.3.20 | L3 | Supplier | The Supplier shall produce and maintain the record of Configuration Items for current equipment, software, and applications architecture and design documentation for issue to the Authority upon request in accordance with Authority's Service Asset and Configuration Management Policies and Processes |
| 7.3.21 | L3 | Supplier | The Supplier shall respond to queries and requests concerning the Configuration Items or supporting information. |
| 7.3.22 | L3 | Supplier | The Supplier shall, if a discrepancy is found with information regarding a Configuration Item, take corrective action to address the discrepancy as directed by the Authority, including:<br>a. identifying any CIs not recorded in the CMDB or incorrectly recorded and adding or correcting such records; and<br>b. reporting on and removing of Authority Assets/CIs that cannot be located, as agreed with the Authority. |
| 7.3.23 | L3 | Supplier | The Supplier shall report any discrepancies in the information regarding a Configuration Item and status of corrective actions taken to the Authority. |
| 7.3.24 | L3 | Supplier | The Supplier shall ensure that the Services delivered, and captured in the Configuration Management Database, are up to date by performing gap analysis of assets catalogued versus any contracted Technology Refresh Service. |
| 7.3.25 | L3 | Supplier | The Supplier shall proactively monitor the expiry of Configuration Items for in scope Services, including licences and tokens, and assist the Other Suppliers and the Authority with keeping the information current. |
| 7.3.26 | L3 | Supplier | The Supplier's responsibilities shall include:<br>a. producing monthly reports that outline a 12 month look ahead to all major software publisher renewals;<br>b. responding in a timely manner to queries and requests concerning the hardware and software asset inventory data or supporting information;<br>c. monitoring for the presence of any unauthorised or non-standard software and remediate where found;<br>d. ensuring that all deployment of software procured by the Authority or the Supplier is compliant with the number of purchased licenses; |

| | | | |
|---|---|---|---|
| | | | e. performing harvesting, de-installation and disposal or re-deployment of equipment and software. Any non-compliance position found shall be remediated where possible by the Supplier via harvesting of under-utilised instances - within one month of the breach being identified or as agreed with the Authority; and<br>f. conducting assurance reviews and audits in accordance with the Configuration Management audit plan and provide evidence to the Authority and its auditors of the accuracy and completeness of the records in the CMDB and the existence of CIs. Where automated validation is not possible, all records shall be validated at least every 12 months. |

## 7.4 Service Catalogue Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.4.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Catalogue Management Policies and Processes. |
| 7.4.2 | L3 | Supplier | The Supplier shall at all times adhere to the Authority's Service Catalogue Management Policies and Processes in the delivery of their Services. The method of update will be agreed with the Authority. |
| 7.4.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Service Catalogue Management Policies and Processes. |
| 7.4.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Service Catalogue Management that are aligned to the Authority's Service Catalogue Management Policies and Processes and shall submit them to the Authority for approval. |
| 7.4.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Service Catalogue Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 7.4.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Service Catalogue Management and report such non-compliance to the Authority. |
| 7.4.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Service Catalogue Management, the Supplier shall bring this to the Authority's attention. |
| 7.4.8 | L3 | Supplier | The Supplier shall be responsible for managing and ensuring the accuracy of its Services and the components within the Products and Service Catalogue, which includes:<br>a. mapping services components into Services and providing accurate information on all Operational Services and those being prepared to be run operationally;<br>b. providing input into the business request catalogue; and<br>c. reviewing the Products and Service Catalogue with all relevant Authority stakeholders. |
| 7.4.9 | L3 | Supplier | The Supplier will ensure that the Supplier services information is available and accurately maintained thereafter within the Products and Services Catalogue (ITSM Product) and Service Portfolio Management. |
| 7.4.10 | L3 | Supplier | The Supplier will ensure that all Products and Services Catalogue items have, at all times, assets and Configuration Items (CIs) identified within the Configuration Management Database (CMDB). |

## 7.5 Release and Deployment Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.5.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Release and Deployment Management Policies and Processes. |
| 7.5.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Release and Deployment Management Policies and Processes in the delivery of their Services. |
| 7.5.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Release Management Policies and Processes. |
| 7.5.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Release and Deployment Management that are aligned to the Authority's Release and Deployment Management Policies and Processes and shall submit them to the Authority for approval. |
| 7.5.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Release and Deployment Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 7.5.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Release and Deployment Management and report such non-compliance to the Authority. |
| 7.5.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Release and Deployment Management, the Supplier shall bring this to the Authority's attention. |
| 7.5.8 | L3 | Supplier | The Supplier shall, as required by the Authority, execute the release and deployment of Operational Changes to the Services into the Production Environment and their component Configuration Items (including software, service management Processes, hardware and associated documentation) and in accordance with the agreed service design package. |
| 7.5.9 | L3 | Supplier | The Supplier shall validate that all items being rolled out or changed are secured in accordance with the Authority Security Document and traceable through the CMDB. |
| 7.5.10 | L3 | Supplier | The Supplier shall resolve all release issues and escalate cross functional issues for resolution, co-ordinate business deployment acceptance Testing and acquire sign-off to retain or back-out. |
| 7.5.11 | L3 | Supplier | The Supplier shall, in accordance with the Authority's Release Management Policies and Procedures, establish and maintain software control and distribution Procedures, including the management of the software Configuration Items and their distribution and implementation into the live service environment. |
| 7.5.12 | L3 | Supplier | The Supplier shall support release impact assessments in support of the Authority's planning and the cross functional release planning. |
| 7.5.13 | L3 | Supplier | The Supplier shall support the release plan, including supporting the business acceptance Testing scope, scripts and resource set out in the Operational Change, sign-off by the Operational Change Management Process. |
| 7.5.14 | L3 | Supplier | The Supplier shall design, build, configure, and Test service rehearsals of the release in conjunction with the Authority and/or the Other Suppliers as necessary. |
| 7.5.15 | L3 | Supplier | The Supplier shall in coordination with the Authority develop and assist in the preparation of release communications and training activities, as agreed with the Authority. |

| | | | |
|---|---|---|---|
| 7.5.16 | L3 | Supplier | The Supplier shall validate that all items being rolled out, or changed, are secured in accordance with the Authority's Information Security Policy and Standards and traceable through the Authority's specified CMDB. |
| 7.5.17 | L3 | Supplier | The Supplier shall resolve all release issues for the Services, escalate cross functional issues for resolution, support business deployment acceptance Testing and acquire sign-off in line with the Authority's Policies and Processes. |
| 7.5.18 | L3 | Supplier | The Supplier shall establish and maintain software control and distribution Procedures, including the management of the software Configuration Items and their distribution and implementation. |
| 7.5.19 | L3 | Supplier | The Supplier shall support release impact assessments in support of the Authority's planning and the cross functional release planning. |
| 7.5.20 | L3 | Supplier | The Supplier shall support the delivery of the release plan. |
| 7.5.21 | L3 | Supplier | The Supplier shall, where required by the Authority and in agreement with the Authority, build and manage Non-Production Environments for services, in line with the Authority's Release and Deployment Management Policy and Processes. |
| 7.5.22 | L3 | Supplier | The Supplier shall provide Testing for all release plans as set out in the relevant Operational Change before they are transferred to the Production Environments including Testing of rollback as described by the agreed back-out plans. |
| 7.5.23 | L3 | Supplier | The Supplier shall conduct a post deployment review of Operational Changes as required by the Authority. |

## 7.6 Demand Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.6.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Demand Management Policies and Processes. |
| 7.6.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Demand Management Policies and Processes in the delivery of the Services. |
| 7.6.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Demand Management Policies and Processes. |
| 7.6.4 | L3 | Supplier | The Supplier acknowledges that, while some demand activities may only affect the Services within the scope of the Supplier, there will be activities that apply to cross-functional services and require cooperation and joint work between the Supplier, the Authority and the Other Suppliers. |
| 7.6.5 | L3 | Supplier | The Supplier shall implement monitoring and reporting of risk indicators of its fulfilment process as needed to monitor trends and emerging risks. |
| 7.6.6 | L3 | Supplier | The Supplier will actively monitor and optimise Service Demand Management to provide optimal value for money, as part of the daily operation of its Services, in accordance with the agreed Demand Management Policies and Processes. |
| 7.6.7 | L3 | Supplier | The Supplier shall provide the Authority with the predicted consumption of the Services on a monthly basis. |
| 7.6.8 | L3 | Supplier | The Supplier shall report to the Authority on patterns of utilisation of the Services from which the Authority can determine patterns of business activity for its Services in scope on a monthly basis. |
| 7.6.9 | L3 | Supplier | The Supplier shall report to the Authority, in a timely manner, the inability to satisfy demand and provide Service Improvement Plans to rectify this inability to satisfy demand. |
| 7.6.10 | L3 | Supplier | The Supplier shall provide Service Demand Management data, status update reports and summary reports at the agreed with the Authority, frequency and in the format agreed with the Authority. |

| | | | |
|---|---|---|---|
| 7.6.11 | L3 | Supplier | The Supplier will provide a report (each Service Reporting Period) that signals consumption increase/decrease (variance) demand for the Services. The report will comprise the following:<br>a. developing Demand Management models;<br>b. recommendations to optimise demands on the Services;<br>c. recommendations on how existing capacity plans for the Services are/will be affected by demand projections; and<br>d. recommendations to the Authority for improvements of the mechanisms to control and meet current and forecast demand for the Services. |
| 7.6.12 | L4 | Authority | The Authority will provide all the necessary information about its business activities and services which is required for the Supplier to perform its obligations in Paragraph 7.6.13. |
| 7.6.13 | L3 | Supplier | The Supplier shall determine, maintain and document patterns of infrastructure consumption by application system activity that, subject to the Authority providing the information set out in paragraph above to enable the Authority to determine business activities. Subject to the Authority providing the information set out in Paragraph 7.6.12 above the Supplier shall identify which services are utilising the resources and to what level, and the schedule of when they must be run and how they correlate to cross-functional services. |
| 7.6.14 | L3 | Supplier | The Supplier shall make recommendations for improvements in the control of demand and the delivery of demand information. |

## 7.7 Service Portfolio Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.7.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Portfolio Management Policies and Processes. |
| 7.7.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Service Portfolio Management Policies and Processes in the delivery of their Services. |
| 7.7.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority 's Service Portfolio Management Policies and Processes. |
| 7.7.4 | L3 | Supplier | The Supplier shall, each Quarter, support the Authority on the review of the service portfolio for its relevant Services, including:<br>a. providing expertise, information, advice and support for the evaluation of existing services and new service opportunities;<br>b. providing expertise, information, advice and support required to prepare a proposal and business case for a new Service or Changes to the Services;<br>c. identifying improvement opportunities for the Services;<br>d. assessing the current state of its Services in the service portfolio; and<br>e. assessing if the Services offered are in line with the Service strategy. |
| 7.7.5 | L4 | Authority | The Authority will, each Quarter, undertake a project to review the Service Portfolio for its relevant Services, including providing expertise, information, guidance and advice for:<br>a. the evaluation of existing Services and new Service opportunities;<br>b. preparing a proposal and business case for a new Service or Changes to existing Service; and |

| | | | |
|---|---|---|---|
| | | | c. the evaluation of retired Services. This may be for re-deployment, for the support of new and existing Services or for removal from the Service Portfolio. |

## 7.8 Financial Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.8.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's IT Financial Management Policies and Processes. |
| 7.8.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Financial Management Policies and Processes in the delivery of their Services. |
| 7.8.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority 's Financial Management Policies and Processes. |
| 7.8.4 | L3 | Supplier | The Supplier shall provide data to assist the Authority in reconciling Charges and invoicing in respect of the Services in accordance with Schedule 7.1 (*Charges and Invoicing*). |
| 7.8.5 | L3 | Supplier | The Supplier shall provide the Authority invoices detailing consumption of the Services in accordance with Schedule 7.1 (*Charges and Invoicing*). |
| 7.8.6 | L3 | Supplier | The Supplier shall assist the Authority in the development and implementation of the consumption reporting and invoicing processes. |
| 7.8.7 | L3 | Supplier | The Supplier shall accurately record and account for all costs and Charges relating to the Services. |
| 7.8.8 | L3 | Supplier | The Supplier shall provide to the Authority all relevant and timely detailed financial information to input into detailed business cases for Changes. |
| 7.8.9 | L3 | Supplier | The Supplier shall provide the Authority on an occasional, ad hoc basis with reasonable assistance with financial forecasting in respect of the Services in support of the Authority's budgeting process. |
| 7.8.10 | L3 | Supplier | The Supplier shall provide reasonable assistance to the Authority in respect of unit prices for Long Term Forecast Business Volumes in response to the future business requirements and business volume forecasts for IT services, provided to the Supplier by the Authority. |
| 7.8.11 | L3 | Supplier | The Supplier shall ensure that each invoice is reconcilable against the Resource Unit (RU) consumption information and is consistent with the content and format agreed between the Authority and Other Suppliers. |
| 7.8.12 | L3 | Supplier | The Supplier shall provide the Authority within ten (10) Working Days after the end of the Service Period with the Management Information on Resource Unit (RU) consumption together with such supporting information as is required for the purposes of validating consumption of the Services and calculating apportionment of the Services consumption across the Authority and related organisations. |
| 7.8.13 | L3 | Supplier | The Supplier shall ensure that information provided is consistent with the content and format agreed with the Authority. |
| 7.8.14 | L3 | Supplier | The Supplier shall cooperate with the Authority and Other Suppliers to answer any questions, to resolve any invoice or consumption dispute and/or any invoice adjustments that may arise in accordance with Schedule 7.1 (*Charges and Invoicing*). |

## 7.9 IT Service Continuity Management (ITSCM)

| Ref | Level | Owner | Description |
|---|---|---|---|
| General | | | |
| 7.9.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's IT Service Continuity Management (ITSCM) Policies and Processes. |
| 7.9.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's ITSCM Policies and Processes in the delivery of the Services. |
| 7.9.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's ITSCM Policies and Processes. |
| 7.9.4 | L3 | Supplier | The Supplier shall provide the Authority with a single point of contact for the ITSCM Plan and provide an escalation process with full contact details. The single point of contact shall be the Supplier Service Director identified as a Key Personnel in Schedule 9.2 (*Key Personnel*). |
| 7.9.5 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for ITSCM that are aligned to the Authority's ITSCM Policies and Processes and shall submit them to the Authority for approval. |
| 7.9.6 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for ITSCM including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 7.9.7 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for ITSCM and report such non-compliance to the Authority. |
| 7.9.8 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the ITSCM Operating Procedures, the Supplier shall bring this to the Authority's attention. |
| 7.9.9 | L3 | Supplier | The Supplier shall ensure the alignment of the ITSCM Strategy, the Service Continuity Plan and the Authority's Business Continuity Plans. |
| 7.9.10 | L3 | Supplier | The Supplier shall provide to the Authority for approval an agreed set of Service Continuity Plans which support the Authority's Business Continuity Plan and are in accordance with the Authority's ITSCM Policies and Processes and the Operating Procedures for ITSCM. |
| 7.9.11 | L3 | Supplier | The Supplier shall design, construct and maintain an Service Continuity Plan, in accordance with the Authority's ITSCM Policies and Processes; the Service Continuity Plan shall include but not be limited to:<br>a. documented plans, Processes, Procedures and communications;<br>b. the Authority's priorities for backups, service continuity, and business continuity based on the priorities established by the Authority;<br>c. flexible methods and timeframes that allow the Authority to change priorities;<br>d. security measures, as defined for normal operations; and<br>e. contact details of key individuals and notification Procedures for the Authority and Other Suppliers. |
| 7.9.12 | L3 | Supplier | The Supplier shall provide all necessary cooperation and assistance to integrate their Service Continuity Plan related to the Services with the service continuity plans of the Other Suppliers, as required by the Authority. |
| 7.9.13 | L3 | Supplier | The Supplier shall provide access upon request to all approved ITSCM Plans to the Other Suppliers and the Authority once they have been approved in writing by the Authority, for distribution via the method and Process agreed with the Authority. |
| 7.9.14 | L3 | Supplier | The Supplier shall continuously maintain the Service Continuity Plan including enhancements required as a result of Changes to the Services. This should include but not be limited to the introduction and use of new technologies |

| | | | |
|---|---|---|---|
| | | | (equipment, software, applications and so forth), Resource Units, processes, business functions, locations and priorities) and from a result of issues identified through Testing the Service Continuity Plans. |
| 7.9.15 | L3 | Supplier | The Supplier shall perform gap analysis of the Service Continuity Plan against Good Industry Practice, regulatory obligations and the Authority's recovery objectives and requirements. The Supplier shall develop rationale and recommendations to address any perceived gaps and make such rationale and recommendations available to the Authority upon request. |
| 7.9.16 | L3 | Supplier | The Supplier shall deploy and implement Processes and Operating Procedures, to ensure operational effectiveness of controls for performing and maintaining:<br>a. viable backups;<br>b. file recovery capabilities; and<br>c. historical archives of files of data and Software (including, where applicable, Object Code) utilised to process data and corresponding records,<br>that can be used to restore the Services to agreed levels in respect of time and with minimum data loss. |
| 7.9.17 | L3 | Supplier | The Supplier shall ensure that, in meeting its additional data and Software backup responsibilities, it shall:<br>a. adhere to the time periods specified for backups and recovery as defined in the IT Service Continuity Plan and regularly, at least annually, performing restore tests on sample backups;<br>b. agree with the Authority an appropriate provision of off-site storage in an agreed secure facility for the back-up data; and<br>c. support connectivity to the Authority's mission-critical production network and the production host systems, or to the contingency network and the recovery sites as required by the IT Service Continuity Plans. |
| 7.9.18 | L3 | Supplier | The Supplier shall provide service continuity testing services, which shall include:<br>a. developing jointly with the Authority, test objectives and success criteria designed to verify that Services and cross functional services will meet the Authority's recovery objectives;<br>b. scheduling and testing all in scope components of the Service Continuity Plans;<br>c. agreeing testing dates with Authority approval, and giving the Authority and its representatives the opportunity to observe and participate in the tests;<br>d. assuming coordination and administrative responsibility during testing in accordance with the Service Continuity Plans and proactively communicating and liaising with the Other Suppliers;<br>e. continuing to operate and manage the Services during periodic IT Service Continuity tests; and<br>f. a demonstration of end to end Service recovery capability including all necessary internal and external interfaces. |
| 7.9.19 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to ensure that end to end testing includes network related failures. |
| 7.9.20 | L3 | Supplier | The Supplier shall perform post-exercise reviews and provide a formal report of the test results. At a minimum, these reports should include:<br>a. a comparison of the results to the measures and goals identified in the respective IT Service Continuity Plan;<br>b. a plan and a schedule, agreed with all the Other Suppliers, to remediate any Service Continuity issues identified during testing; and<br>c. such plans may include additional walkthroughs, scenario tests, partial tests |

| | | | |
|---|---|---|---|
| 7.9.21 | L3 | Supplier | The Supplier shall continuously maintain the IT Service Continuity Plan including enhancements required as a result of Changes to the Services, and from a result of issues identified through testing the IT Service Continuity Plans. |
| 7.9.22 | L3 | Supplier | The Supplier shall, in the event of the invocation of local business continuity plans, manage any request for replacement and installation of equipment within timescales agreed with the Authority. |
| 7.9.23 | L3 | Supplier | The Supplier shall define with the Authority clear and unambiguous triggers and closure points relating to ITSCM Events. |
| 7.9.24 | L3 | Supplier | The Supplier shall report Disasters (or potential disasters) immediately upon identification based on parameters defined in the IT Service Continuity Plans and consult with the Authority for an official declaration of a Disaster as appropriate. |
| 7.9.25 | L3 | Supplier | The Supplier shall in the event of a Disaster:<br>a. provide such immediate assistance and increased support as requested in relation to the management, containment and/or resolution of any disaster;<br>b. execute the Service Continuity Plans as directed by the Authority and IT Operation Centre;<br>c. provide additional resources as necessary to maintain provision of the Services for unaffected areas; and<br>d. verify full recovery of the Services and that this has been implemented in accordance with the Service Continuity Plan. |
| 7.9.26 | L3 | Supplier | The Supplier shall, following any Disaster, conduct a post-Disaster review with the Authority in order to understand the cause of the Disaster and develop plans to eliminate or mitigate future occurrences. Such review may include an audit to be carried out as requested by the Authority. |
| 7.9.27 | L3 | Supplier | The Supplier shall, following any Disaster conduct a post-Disaster review with the Authority in order to develop the Service Continuity Plan. |
| 7.9.28 | L3 | Supplier | The Supplier shall provide, on request by the Authority, an ITSC awareness and training plan for ITSC related staff. |
| 7.9.29 | L3 | Supplier | The Supplier shall undertake an annual review of the ITSCM Plan within thirty (30) days of each annual test. |
| 7.9.30 | L3 | Supplier | Between annual reviews, the Supplier shall update the ITSCM Plan to reflect any Changes agreed thereto between the Parties. |
| 7.9.31 | L3 | Supplier | The Supplier shall agree with the Authority a schedule for completing regular business impact analysis (BIA) exercises to ensure that all ITSCM Plans are maintained in line with changing business impacts and requirements. |
| 7.9.32 | L3 | Supplier | Where the Authority has declared the occurrence of an ITSCM Event, the Supplier shall comply with the obligations pursuant to the sections of the ITSCM Plan applicable to the ITSCM Event in question. |
| 7.9.33 | L3 | Supplier | The Supplier shall where appropriate, recommend to the Authority the invocation of an ITSCM Event in accordance with the ITSCM Plan and Authority's IT Service Continuity Policies and Processes |
| 7.9.34 | L3 | Supplier | Where relevant and instructed by the Authority, the Supplier shall provide such information, guidance and assistance as may be reasonably requested by the Authority within such timeframes as may be reasonably requested to assist it in the production of the Normal Service restoration plan. |
| 7.9.35 | L3 | Supplier | The Supplier shall, following agreement of any Normal Service restoration plan, comply with the obligations pursuant to such Normal Service restoration plan. |
| 7.9.36 | L3 | Supplier | The Supplier shall, prior to closure of an ITSCM Event, assist with and participate in the Authority's planning of action required to restore Normal Service. |
| 7.9.37 | L3 | Supplier | The Supplier shall inform the Authority when the Supplier believes that an ITSCM Event should be closed. |

| | | | |
|---|---|---|---|
| 7.9.38 | L3 | Supplier | The Supplier shall, where relevant, provide such information, guidance and assistance as may be reasonably requested within such timeframes as may be reasonably requested to assist it in the production of the Normal Service Restoration Plan within thirty (30) days of the date of the declaration by the Authority of the occurrence of an ITSCM Event (unless, Normal Service has been resumed within such thirty (30) day period). |
| 7.9.39 | L3 | Supplier | The Supplier shall collaborate, where required, with the Authority and Other Suppliers in the production of the ITSCM Event Closure Report. |
| 7.9.40 | L3 | Supplier | The Supplier shall monitor the elements of the ITSCM Plan relating to the Services; and identify emerging risks to the continuity of the provision of the Services by the Supplier. |
| 7.9.41 | L3 | Supplier | The Supplier shall advise the Authority in writing of any emerging risks to the continuity of the provision of the Services identified by the Supplier together with a proposal of how such emerging risks should be addressed. |

## 7.10 Architecture and Strategy

| Ref | Level | Owner | Description |
|---|---|---|---|
| 7.10.1 | L3 | Supplier | The Supplier shall at all times conform to Good Industry Practice for enterprise Architecture Management and shall align to the Government Digital Services (GDS) Technology Code of Practice, in the delivery of their Services. |
| 7.10.2 | L3 | Supplier | The Supplier shall provide reasonable assistance to the Authority in the development of the Enterprise IT Architecture Level 1 Architecture documentation. |
| 7.10.3 | L3 | Supplier | The Supplier shall ensure that the Services architecture conforms to the Technical Framework Document and/or successor Technical Framework Document. |
| 7.10.4 | L3 | Supplier | The Supplier shall architect, develop and provide integration of the Supplier's toolsets to the Authority's specified service integration and management capability. |
| 7.10.5 | L3 | Supplier | Use a proven, recognised, industry standard software engineering life cycle methodology to analyse, design, construct, Test and implement security controls in new software information systems. |
| 7.10.6 | L3 | Supplier | The Supplier shall compile a summary of compliance / non-compliance reports for the Authority, as agreed. |
| 7.10.7 | L3 | Supplier | The Supplier shall implement the remediation actions necessary to resolve the non-compliances set out in Paragraph 7.10.6 above as agreed with the Authority. |
| 7.10.8 | L3 | Supplier | The Supplier shall work with the Authority and Other Suppliers to identify any Services or services of Other Suppliers that can be combined to form higher-value services. |
| 7.10.9 | L3 | Supplier | The Supplier shall assist the Authority in developing and updating the long-range, comprehensive plan for the Authority's integrated services, IT Systems, processes, technical architecture and standards (the "Long-Range IT Plan"). While the Authority will be primarily responsible for this plan, the Supplier shall serve as a key collaborator. The "Long-Range IT Plan" will be developed on an annual basis and shall include a rolling three (3) year projection of anticipated changes (subject to the Authority business and planning requirements). |
| 7.10.10 | L3 | Supplier | The Supplier shall provide Enterprise IT Architecture Level 2 documents that address:<br>a. Architecture overview;<br>b. LAN and WAN architecture;<br>c. IP telephony architecture;<br>d. OSS architecture; and<br>e. Security architecture. |

| | | | |
|---|---|---|---|
| 7.10.11 | L3 | Supplier | The Supplier shall support the Authority by providing and communicating information regarding:<br>a. equipment and Software;<br>b. architecture and relevant standards;<br>c. industry and technology trends;<br>d. regulatory issues/changes where they are aware of such issues/changes;<br>e. data and lessons learned from the Operating Environment;<br>f. trend analysis from resource and consumption data to predict future demand;<br>g. good practice from their other accounts and centres of excellence; and<br>h. any element of the infrastructure or architecture which is forecast to go "End of Life" within the following 12 months. |
| 7.10.12 | L3 | Supplier | The Supplier shall assess potential changes to the Authority's architecture and maintain Architecture Standards requirements and allowable exceptions, including notifying the Authority of any changes to the Supplier's own architecture and standards applicable to the Services. |
| 7.10.13 | L3 | Supplier | The Supplier shall ensure that all changes comply with agreed Architecture Standards. If required by the Authority, the Supplier shall produce a summary of compliance / non-compliance Architecture Standards reports. |
| 7.10.14 | L3 | Supplier | The Supplier shall inform the Authority promptly of any non-compliance with agreed Architecture Standards. |
| 7.10.15 | L3 | Supplier | The Supplier shall implement, track and report on agreed remediation actions in respect of any non-compliance with agreed Architecture Standards. |
| 7.10.16 | L3 | Supplier | The Supplier shall, at the request of the Authority:<br>a. participate in evaluations and Testing equipment, software, and related products or the Services prior to their use or deployment in the Authority's Production Environment;<br>b. participate in evaluations involving new third party products and services which may be used in the provision of the Services; and<br>c. upon request, provide reports, summaries, or results of its evaluation and Testing of third party products and services which may be used in the provision of the Services. |

# 8. Service Knowledge Management

## 8.1 General

| Ref | Level | Owner | Description |
|---|---|---|---|
| 8.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Knowledge Management Policies and Processes. |
| 8.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Knowledge Management Policies and Processes in the delivery of their Services. |
| 8.1.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority 's Knowledge Management Policies and Processes. |
| 8.1.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Knowledge Management that are aligned to the Authority's Knowledge Management Policies and Processes and shall submit them to the Authority for approval. |
| 8.1.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Knowledge Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 8.1.6 | L3 | Supplier | The Supplier shall monitor the compliance and take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Knowledge Management and report non-such compliance to the Authority. |
| 8.1.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Knowledge Management, the Supplier shall bring this to the Authority's attention. |
| 8.1.8 | L3 | Supplier | The Supplier shall provide, maintain and make available to the Authority and all Other Suppliers the Service Knowledge including but not limited to:<br>a. knowledge identification and capture;<br>b. knowledge transfer;<br>c. data and information management;<br>d. evaluation, update, improvement and governance;<br>e. audit; and<br>f. editorial ownership. |

## 8.2 Service Knowledge Management System (SKMS)

| Ref | Level | Owner | Description |
|---|---|---|---|
| 8.2.1 | L3 | Supplier | The Supplier shall deploy and maintain a Service Knowledge Management System (SKMS) for the capture, storage, and presentation of the information required to manage the Services. The SKMS shall contain data and information, including but not limited to:<br>a. Methods to resolve Incidents;<br>b. Known Errors;<br>c. Service Desk scripts; |

| | | | |
|---|---|---|---|
| | | | d. Self help articles; and<br>e. Frequently asked questions (FAQs). |
| 8.2.2 | L3 | Supplier | The Supplier shall, for the SKMS:<br>a. establish data and information requirements;<br>b. define the information schema; and<br>c. establish data and Information Management Procedures. |
| 8.2.3 | L3 | Supplier | The Supplier shall ensure the SKMS is integrated into the CMDB and other relevant information systems. |
| 8.2.4 | L3 | Supplier | The Supplier shall make the SKMS available to the Authority and the Other Suppliers to review, update and utilise SKMS processes, data and information. |
| 8.2.5 | L3 | Supplier | The Supplier shall conduct regular assurance activities to ensure information required to manage the Services is captured, stored, and presented accurately and completely in the Service Knowledge Management System (SKMS). |
| 8.2.6 | L3 | Supplier | The Supplier shall, at all times, update the ITSM Product and Service Knowledge Management System (SKMS) immediately as new knowledge, Authority Assets, knowledge articles, Known Errors, FAQs, guidance and other items are produced in support of Other Supplier and Authority Processes and services. |
| 8.2.7 | L3 | Supplier | The Supplier shall cooperate with the Authority to carry out conformance reviews and audits to ensure the integrity and accuracy of data in the Service Knowledge Management System (SKMS) |
| 8.2.8 | L3 | Supplier | When data is found in the SKMS that is inaccurate, incomplete or lacks integrity, the Supplier shall ensure such data is corrected or removed. |
| 8.2.9 | L3 | Supplier | The Supplier shall, promptly following the end of each Service Period provide the Authority with a comprehensive list of all new knowledge articles for the preceding Service Period. |
| 8.2.10 | L3 | Supplier | The Supplier shall support the Authority with periodic verification of the Service Knowledge Management System (SKMS) contents to ensure the currency of the data and information contained therein. |
| 8.2.11 | L3 | Supplier | The Supplier shall provide and make available appropriate education, skills, knowledge and training to the Authority and the Other Suppliers in how to utilise the SKMS. |
| 8.2.12 | L3 | Supplier | The Supplier shall manage and execute an on-going knowledge transfer process in preparation for complying with the relevant Exit Management provision in this Agreement. |
| 8.2.13 | L3 | Supplier | The Supplier shall ensure that the information in the master Site list is maintained and managed within the Service Knowledge Management System. References to the master Site list shall include any replacement list, managed by or on behalf of the Authority for the same purpose. |

# 9. Service Level Management

## 9.1 Management and Reporting

| Ref | Level | Owner | Description |
|---|---|---|---|
| 9.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Level Management Policies and Processes. |
| 9.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Service Level Management Policies and Processes in the delivery of their Services. |
| 9.1.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority 's Service Level Management Policies and Processes. |
| 9.1.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Service Level Management that are aligned to the Authority's Service Level Management Policies and Processes and shall submit them to the Authority for approval. |
| 9.1.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Service Level Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 9.1.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Service Level Management and report such non-compliance to the Authority. |
| 9.1.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Service Level Management, the Supplier shall bring this to the Authority's attention. |
| 9.1.8 | L3 | Supplier | The Supplier shall gather performance data, in accordance with the Target Performance Levels and Performance Indicators in Schedule 2.2 (*Performance Levels*) that report performance against Target Performance Levels, the content and format of which will be agreed with the Authority:<br>a. reporting against data gathered;<br>b. provide raw data underpinning reports; and<br>c. populate the Service Level Management tooling with service measurement data. |
| 9.1.9 | L3 | Supplier | The Supplier shall implement monitoring and reporting of risk indicators of the Service Level Management Process as needed to monitor trends and emerging risks. |
| 9.1.10 | L3 | Supplier | The Supplier shall deliver operational reports and dashboards, including performance management reports, in accordance with the provisions of this Agreement. |
| 9.1.11 | L3 | Supplier | The Supplier shall collaborate with its own service management functions to determine detailed requirements for reporting. |
| 9.1.12 | L3 | Supplier | The Supplier shall ensure on-time delivery of all the Supplier performance management reports, in accordance with the timelines defined by, and agreed with the Authority, including those set out in Schedule 2.2 (*Performance Levels*). |
| 9.1.13 | L3 | Supplier | The Supplier shall deliver a Target Performance Level audit trail in a format agreed with the Authority to enable data mining of Performance Indicator data. |
| 9.1.14 | L3 | Supplier | The Supplier shall advise the Authority in writing and review with them, each material non-compliance in accordance with Clause 7 (*Performance Indicators*) and Schedule 2.2 (*Performance Levels*). |

| | | | |
|---|---|---|---|
| 9.1.15 | L3 | Supplier | The Supplier shall address each such material non-compliance with an agreed Rectification Plan in order to avoid further non-compliance in accordance with Clause 7 (*Performance Indicators*) and Schedule 2.2 (*Performance Levels*). |
| 9.1.16 | L3 | Supplier | The Supplier shall:<br>a. handle inaccuracies, questions and issues arising from the provision of Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*) reporting and/or data;<br>b. check reported Performance Indicators and Knowledge Management performance against the Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*).<br>c. perform trend and current performance analysis;<br>d. ensure that agreed collection tools are used; and<br>e. escalate issues to governance for attention, discussion and resolution. |
| 9.1.17 | L3 | Supplier | The Supplier shall monitor and report its individual performance against agreed Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*) and take corrective action, as required by the provisions of this Agreement, when any deviations are observed. |
| 9.1.18 | L3 | Supplier | Where appropriate, the Supplier shall, as directed by its own service management functions, agree and execute Operating Level Agreements (OLAs) with Other Suppliers, with the aim of the Supplier and the Other Suppliers achieving the end to end Performance Indicators. The Supplier shall monitor performance against agreed OLAs and shall provide OLA performance reporting to the Authority. |
| 9.1.19 | L3 | Supplier | The Supplier shall support its own service management functions in the completion of cross functional Service Reviews with representatives of the Authority and Other Suppliers. |
| 9.1.20 | L3 | Supplier | The Supplier shall support in maintaining and improving business-aligned service quality through a constant cycle of agreeing, monitoring, reporting and reviewing Service provision and through instigating improvement actions to eradicate unacceptable levels of Target Performance Level performance within the Services. |
| 9.1.21 | L3 | Supplier | The Supplier shall address emerging or current Target Performance Level performance issues by delivering improvement actions. |
| 9.1.22 | L3 | Supplier | The Supplier shall deliver to agreed action plans for improvements to address emerging or current Target Performance Level performance issues. |

# 10. Continual Service Improvement (CSI) Management

## 10.1 Continual Service Improvement

| Ref | Level | Owner | Description |
|---|---|---|---|
| 10.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Continual Service Improvement (CSI) Management Policies and Processes. |
| 10.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's CSI Management Policies and Processes in the delivery of their Services. |
| 10.1.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's CSI Management Policies and Processes. |
| 10.1.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for CSI Management that are aligned to the Authority's CSI Management Policies and Processes and shall submit them to the Authority for approval. |
| 10.1.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for CSI Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 10.1.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for CSI Management and shall report such non-compliance to the Authority. |
| 10.1.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for CSI Management, the Supplier shall bring this to the Authority's attention. |
| 10.1.8 | L3 | Supplier | The Supplier shall ensure that baseline data is captured within one hundred and eighty (180) calendar days of the Effective Date to measure the effectiveness of all improvements across the Services. |
| 10.1.9 | L3 | Supplier | The Supplier shall develop within three (3) months of the baseline data being captured, and maintain thereafter, its own Service Improvement Plans (SIPs) with measurable improvement targets and provide its plans to the Authority for review and acceptance. |
| 10.1.10 | L3 | Supplier | The Supplier shall provide regular CSI reporting during each Service Period. |
| 10.1.11 | L3 | Supplier | The Supplier shall, where agreed with the Authority, support information exchange between and among the Authority and the Other Suppliers to support the objectives of Continual Service Improvement (CSI) management. |
| 10.1.12 | L3 | Supplier | The Supplier shall analyse monitoring results to identify areas of the overall configuration that could be tuned or optimised, to better utilise the Service, system and component resources or improve the performance of the particular Service. |
| 10.1.13 | L3 | Supplier | The Supplier shall support organisational change programmes to support new ways of working, improve productivity and maximise business efficiency and to assist the Authority in moving in accordance with any agreed tactical or strategic plans. |
| 10.1.14 | L3 | Supplier | The Supplier shall review industry and business conditions, leverage the Supplier's experience in other engagements, and assess developments in best-practice and technology to identify opportunities that these may offer if adopted. |
| 10.1.15 | L3 | Supplier | The Supplier shall cooperate with the Authority and Other Suppliers, on Continual Service Improvement activities across the Services. |

| | | | |
|---|---|---|---|
| 10.1.16 | L3 | Supplier | The Supplier shall support the Authority and Other Suppliers, with the prioritisation of improvement opportunities across the Services. |
| 10.1.17 | L3 | Supplier | The Supplier shall provide suggestions and plans regarding agreed improvement targets that have not been achieved, in line with the Authority's Continual Service Improvement Management Policies and Processes. |
| 10.1.18 | L3 | Supplier | The Supplier shall manage the implementation of its improvement plans to deliver improvement targets as agreed. |
| 10.1.19 | L3 | Supplier | The Supplier shall identify and develop a set of measures that are relevant to its Services which support the identification of effective improvement. |
| 10.1.20 | L3 | Supplier | The Supplier shall identify candidates and requirements for the deployment of new technology or the automation of tasks associated with the Services. |
| 10.1.21 | L3 | Supplier | The Supplier shall proactively seek to automate manual tasks associated with the Services, advise the Authority of such opportunities and implement such opportunities where agreed with the Authority. |
| 10.1.22 | L3 | Supplier | The Supplier shall promote, engage and encourage active cross-functional, cross-group, and cross-location coordination and communication related to new technology and automation that may be of benefit to the Authority. |
| 10.1.23 | L3 | Supplier | The Supplier shall proactively identify strategies, approaches and innovations for future IT service delivery that the Supplier believes will provide the Authority with competitive advantages and that may result in increased efficiency, effectiveness, performance, or cost savings. |
| 10.1.24 | L3 | Supplier | The Supplier shall gather and incorporate the data and lessons learned from the Operating Environment that may impact Continual Service Improvement (CSI) plans. |
| 10.1.25 | L3 | Supplier | The Supplier shall perform trend analysis from the resource consumption data to project future demand that may impact CSI planning activities. |
| 10.1.26 | L3 | Supplier | Where any failure which is under the control of the Supplier has a direct operational impact on the Authority, , the Supplier shall apply a Service Improvement Plan initiative immediately. The Supplier shall ensure that the Service Improvement Plan includes, as a minimum, the following stages:<br>a. criticality assessment (including risk and threat Assessment);<br>b. gathering of information;<br>c. detailed analysis of information leading to failure determination;<br>d. action plan;<br>e. preventative reoccurrence measures;<br>f. implementation plan;<br>g. executive (where required) and technical reports; and<br>h. portfolio of evidence to substantiate the process. |

# 11. Service Design - Information Security Management

## 11.1 Information Security Management Support

| Ref | Level | Owner | Description |
|---|---|---|---|
| 11.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Information Security Management Policies and Processes. |
| 11.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Information Security Policy and Standards in the delivery of their Services. |
| 11.1.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Information Security Management Policies and Processes. |
| 11.1.4 | L3 | Supplier | The Supplier shall manage transition and transformation activities in compliance with the Authority's Information Security Policy and Standards. |
| 11.1.5 | L3 | Supplier | The Supplier shall provide support to the Authority's Security Operations Centre (SOC) Supplier to ensure the confidentiality, integrity, availability and authenticity of information, data and IT services within the Services. |

# 12. Service Transition

## 12.1 Transition Planning and Support (per agreed transition)

| Ref | Level | Owner | Description |
|---|---|---|---|
| 12.1.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Transition Management Policies and Processes. |
| 12.1.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Service Transition Management Policies and Processes in the delivery of the Services. |
| 12.1.3 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Service Transition Management that are aligned to the Authority's Service Transition Management Policies and Processes and shall submit them to the Authority for approval. |
| 12.1.4 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Service Transition Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 12.1.5 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Service Transition Management and report such non-compliance to the Authority. |
| 12.1.6 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Service Transition Management, the Supplier shall bring this to the Authority's attention. |
| 12.1.7 | L3 | Supplier | The Supplier shall execute the operational readiness Process as defined in the Authority's Service Transition Management Policies and Processes and in the Authority's Release Management Policy and Processes for each Project requiring transfer from development through to production and operational support where such process requires involvement of Other Suppliers as necessary to deliver, support and maintain the Services. |
| 12.1.8 | L3 | Supplier | The Supplier shall establish and maintain an operational Process that delivers the Authority's Service Transition Services in a coordinated manner. |
| 12.1.9 | L3 | Supplier | The Supplier shall establish and maintain an operational readiness framework for use during acceptance for go-live. |
| 12.1.10 | L3 | Supplier | The Supplier shall, in collaboration with the Authority and where appropriate the Other Suppliers, develop Service Transition plans that describe the tasks and activities to roll out a release in development, Test and Production Environments and that includes resource allocation and risk/issue management. The Service Transition plan is subject to approval by the service management functions and the Authority. |
| 12.1.11 | L3 | Supplier | The Supplier shall define the lifecycle stages for the Service Transition, and the move from one stage to the next shall be subject to formal checks. Typical stages in the life of a transition shall include, but are not limited to all of:<br>a. acquire and Test new Configuration Items (CIs) and components;<br>b. build and release Test;<br>c. service release Test;<br>d. service operational readiness Test; and<br>e. review and close Service Transition. |

| | | | |
|---|---|---|---|
| 12.1.12 | L3 | Supplier | The Supplier shall work with the service designers to provide advice and assistance in understanding the Service Transition Management Policies and Processes and in completing the relevant documentation, such as the service design package. |
| 12.1.13 | L3 | Supplier | The Supplier shall ensure all reviewing and checking of the input deliverables, for example, Operational Change proposal, service design package, service acceptance criteria and evaluation report. |
| 12.1.14 | L3 | Supplier | The Supplier shall work with the Authority and Other Suppliers to define the Service Transition responsibilities and deliverables matrices, subject to Authority approval. |
| 12.1.15 | L3 | Supplier | The Supplier shall develop Service Transition plans which integrate into a cross functional service transition plan with Other Suppliers implementing the service design package that describes the tasks and activities to roll out a release into development, Test and Production Environments and that includes resource allocation and risk/issue management, subject to approval by the Authority. |
| 12.1.16 | L3 | Supplier | The Supplier shall support the Authority and Other Suppliers with communications throughout the Service Transition for the Services. |
| 12.1.17 | L3 | Supplier | The Supplier shall support agile development and operational support in alignment with Government Digital Service (GDS) standards. |
| 12.1.18 | L3 | Supplier | The Supplier shall monitor and report in scope Service Transition activities against the intentions set out in the transition model and plan. The Supplier will provide regular status updates to the Authority as required. |
| 12.1.19 | L3 | Supplier | The Supplier will provide a full and complete service handover pack to the Authority covering all the aspects necessary to undertake effective management, delivery and support to the use and consumption of the Supplier service by the Authority and ensure that this is available via the Service Knowledge Management module (within the ITSM Product) and associated artefacts captured and available within the CMDB . |

## 12.2 Service Validation and Testing

| Ref | Level | Owner | Description |
|---|---|---|---|
| 12.2.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Service Validation and Testing Policies and Processes. |
| 12.2.2 | L3 | Supplier | The Supplier shall, at all times, adhere to the Authority's Service Validation and Testing Policies and Processes and the Schedule 6.2 (Testing Procedures).in the delivery of the Services. |
| 12.2.3 | L3 | Suppliers | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Service Validation and Testing Policies and Processes. |
| 12.2.4 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Service Validation and Testing Management that are aligned to the Authority's Service Validation and Testing Management Policies and Processes and shall submit them to the Authority for approval. |
| 12.2.5 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Service Validation and Testing Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 12.2.6 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Service Validation and Testing Management and report such non-compliance to the Authority. |

| | | | |
|---|---|---|---|
| 12.2.7 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Service Validation and Testing Management, the Supplier shall bring this to the Authority's attention. |
| 12.2.8 | L3 | Supplier | The Supplier will ensure all Testing conducted complies with Schedule 6.2 (Testing Procedures). |
| 12.2.9 | L3 | Supplier | The Supplier shall maintain Test Environments, as agreed with the Authority, to such a state that they match that running in the Authority's Production Environment and ensure all interfaces between Test platforms under the control of the Supplier are fully functional. |
| 12.2.10 | L3 | Supplier | The Supplier shall where required assist in the preparation and loading of agreed Test data or suitably masked live data into the Test Environments and remove the data from those environments once Testing is complete. |
| 12.2.11 | L3 | Supplier | The Supplier shall support the resolution of platform integration-related issues with the relevant Other Suppliers. |
| 12.2.12 | L3 | Supplier | The Supplier will support the Authority to develop and extend Schedule 6.2 (Testing Procedures) following lessons learned from Implementation and any Projects or Operational Change Request thereafter. |
| 12.2.13 | L4 | Authority | The Authority will perform Test assurance activities. Such assurance activities do not diminish the Supplier's obligations in relation to Testing or meeting the Target Performance Levels. |
| 12.2.14 | L3 | Supplier | The Supplier shall support the Authority (where required) in the planning, design, implementation, execution and reporting of User Acceptance Testing (UAT). |

## 12.3 Software Licence and Asset Management

| Ref | Level | Owner | Description |
|---|---|---|---|
| 12.3.1 | L4 | Authority | The Authority shall maintain and make available to the Supplier the Authority's Software Asset Management Policies and Processes. |
| 12.3.2 | L3 | Supplier | The Supplier shall comply with the Authority's agreed Software Management Policies and Processes. |
| 12.3.3 | L3 | Supplier | The Supplier shall work with the Authority and the Other Suppliers to implement the Authority's Software Asset Management Policies and Processes. |
| 12.3.4 | L3 | Supplier | The Supplier shall administer, support and control the Software Asset Management Policies and Processes including the acquisition (where requested by the Authority), documentation, distribution and installation, usage and retirement of software assets, in accordance with the relevant software licence agreements and in accordance with the Technical Framework Document. |
| 12.3.5 | L3 | Supplier | The Supplier shall define and maintain Operating Procedures for Software Asset Management that are aligned to the Authority's Software Asset Management Policies and Processes and the Technical Framework Document and shall submit them to the Authority for approval. |
| 12.3.6 | L3 | Supplier | The Supplier shall provide the management for all editorial activities with regards to the Operating Procedures for Software Asset Management including but not limited to content creation, update, change control and circulation across Other Suppliers. |
| 12.3.7 | L3 | Supplier | The Supplier shall monitor the compliance and shall take all reasonable steps to address any non-compliance of the Other Suppliers against the Operating Procedures for Software Asset Management and report such non-compliance to the Authority. |

| | | | |
|---|---|---|---|
| 12.3.8 | L3 | Supplier | Where the Supplier is unable to address the non-compliance of any Other Supplier to the Operating Procedures for Software Asset Management, the Supplier shall bring this to the Authority's attention. |
| 12.3.9 | L3 | Supplier | The Supplier will use the Supplier's IT Asset Management (ITAM) solution to support the agreed Software Asset Management Policies and Processes. |
| 12.3.10 | L3 | | The Supplier shall, where there are gaps in the functionality of the Supplier's existing tools and software to support the Software Asset Management Policies and Processes, agree with the Authority how these gaps will be addressed. |
| 12.3.11 | L3 | Supplier | The Supplier shall provide and enter the data into the Authority's specified ITAM solution for:<br>a. purchasing of all software assets;<br>b. optimisation of the software asset purchasing process;<br>c. deployment of all software assets on the Authority's estate;<br>d. maintenance of the software assets on the Authority's estate;<br>e. monitoring the utilisation of the software assets;<br>f. optimising the utilisation of the software assets; and<br>g. tracking of licence expiration and advising the Authority accordingly disposal of software assets. |
| 12.3.12 | L3 | Supplier | The Supplier will work with the Authority to minimise the costs associated with the deployment and operation of software assets by automating its processes wherever possible, in particular (though not limited to) those associated with inventory tracking, issue tracking, patch management, software deployment and configuration compliance. |
| 12.3.13 | L3 | Supplier | Each Service Period, the Supplier shall review all licence deficiencies and provide a software licence compliance report in the format specified by the Authority. |
| 12.3.14 | L3 | Supplier | Each Service Period, the Supplier shall remediate any licence deficiencies identified in the software licence compliance report identified in Paragraph 12.3.14 above, which relate to any licences that the Supplier acquires on behalf of the Authority, including any ITSM Product related licences. |
| 12.3.15 | L3 | Supplier | The Supplier 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 Policies and Processes and the Technical Framework Document. |
| 12.3.16 | L3 | Supplier | The Supplier shall ensure that all necessary support is provided to any Auditor or any external licence audits requested by the Authority or authorised third parties. |
| 12.3.17 | L3 | Supplier | The Supplier shall provide appropriate auditing tools including software licensing in support of Software licence Management. |
| 12.3.18 | L3 | Supplier | The Supplier shall proactively monitor the use of all Software in order to maintain strict compliance, such monitoring activities to include:<br>a. immediately notifying and advising the Authority of any Software licence compliance issues identified within the Authority's IT Environment or associated with the use of or support of the Services provided to the Authority;<br>b. monitoring all software associated with the Services, ensure appropriate provisioning and availability of Software;<br>c. ensuring appropriate monitoring is put in place for the purposes of identifying the presence of any unauthorised or non-standard Software;<br>d. providing periodic reporting of license information and compliance to Authority, as required; and<br>e. filing and tracking Software license agreements in the Service Portfolio and ensuring appropriate links within the CMDB, the asset register and Definitive Media Library. |

| | | | |
|---|---|---|---|
| 12.3.19 | L3 | Supplier | The Supplier shall, every six months following the Effective Date, undertake a review to identify any software currently in use which is not at the agreed release level and propose a strategy to Upgrade to the agreed release level. |
| 12.3.20 | L3 | Supplier | The Supplier shall ensure that the CMDB is kept up to date with licence information in line with the relevant Authority Policies and Procedures. |
| 12.3.21 | L3 | Supplier | The Supplier shall maintain accurate and up to date records of all licences provided by the Supplier for use of the Services and of all licences for hardware and software used by the Supplier in the provision of the Services to the extent that such licences were maintained by the Supplier at the Effective Date. |
| 12.3.22 | L3 | Supplier | The Supplier shall provide the Authority with access to the records of such licences. |

# 13. Solution Testing and Transition

## 13.1 User Acceptance Testing (UAT)

| Ref | Level | Owner | Description |
|---|---|---|---|
| 13.1.1 | L3 | Supplier | The Supplier shall support the delivery of User Acceptance Testing (UAT) in line with Schedule 6.2 (Testing Procedures).. |

## 13.2 Operational Acceptance Testing (OAT)

| Ref | Level | Owner | Description |
|---|---|---|---|
| 13.2.1 | L3 | Supplier | The Supplier shall produce a proposed operational acceptance Test (OAT) strategy for each Project, (including Test Success Criteria and a Test plan) and include it in the Project Test Strategy which shall adhere to Schedule 6.2 (Testing Procedures). |
| 13.2.2 | L3 | Supplier | The Supplier shall discuss and agree each proposed OAT strategy within the Project Test Strategy with the Authority's nominated Project or service lead. |
| 13.2.3 | L3 | Supplier | The Supplier shall perform OAT for each Project in accordance with the agreed Project Test Strategy. |
| 13.2.4 | L3 | Supplier | The Supplier shall provide an OAT report to the Authority no later than one week after completion of the OAT for each activity which includes details as to whether the Supplier would accept (together with details of any qualifications attaching to such acceptance) or reject the solution Tested for installation into the Live Environment. |
| 13.2.5 | L3 | Supplier | The Supplier shall provide clarifications about any OAT report to the Authority as reasonably requested. |

## 13.3 Service Acceptance Testing (SAT)

| Ref | Level | Owner | Description |
|---|---|---|---|
| 13.3.1 | L3 | Supplier | The Supplier shall discuss and agree with the Authority the service acceptance Test (SAT) strategy in respect of each Project (including Test Success Criteria and Project Test Plan) and shall include it in the Project Test Strategy in accordance with the Project Implementation Plan. |
| 13.3.2 | L4 | Authority | The Authority shall provide the Supplier with the SAT Test Success Criteria and associated relevant strategies and Project Test Plans applicable to each Project. |
| 13.3.3 | L3 | Supplier | The Supplier shall perform SAT in accordance with the agreed Project Test Strategy and the Project Implementation Plan. |
| 13.3.4 | L4 | Authority | The Authority shall provide required information necessary to allow the Supplier to perform SAT. |
| 13.3.5 | L3 | Supplier | The Supplier shall support the preparation of information related to the provision of the Services which is required by the Authority for the Gated Review Process. |