SERVICE INTEGRATION AND MANAGEMENT (SIAM) PROCESS FRAMEWORK

Version: 0.1

Owner: Head of SIAM

Date: 27 April 2017

DOCUMENT CHANGE HISTORY

Version	Date	Editor	Description of Change
0.1	27 April 2017		Initial outline document

CONTRIBUTORS

Name	Role	Author / Review / Approve

TABLE OF CONTENTS

1 OVERVIEW

1.1 Description

- This document provides an overview of the organisation's Service Integration and Management (SIAM) process framework. It provides details of the target service operating mode (TSOM), the functional groups that make up the TSOM, boundaries of responsibility and detailed resposibilities for each process.
- The document includes a set of guiding principles or rules, intended to influence all service integration process activity across the organisation, the service integrator and service providers. They include:
  - Formally documented management expectations and intentions, used to direct decisions and ensure consistent and appropriate development and implementation of processes, roles and activities.
  - Guiding principles used to set direction in a process, to guide and influence decisions.
  - Basic concepts and/or key assumptions with respect to areas of possible contention to ensure all key stakeholders are 'on the same page'.
- All staff across the organisation, the service integrator and service providers must adhere to the requirements of this document, whilst executing the related processes and procedures.
- This document should be:
  - Reviewed on an annual basis by the Head of SIAM or upon request of the IT leadership team.
  - Evolved over time through a continual service improvement approach.
- This document covers the three core parties: the organisation, service integrator and service providers. To ensure nothing gets missed, it is often prudent to ensure that all core process activities are considered.
- Note that the process overviews included in this document have been defined at a detailed level to ensure that nothing gets missed.

1.2 Revision

The Head of SIAM owns this document and is responsible for keeping it current. This document will be reviewed annually or as circumstances arise.

An internal audit will be regularly performed to ensure that the document is properly aligned with company objectives and that performance is meeting established parameters.

1.3 Exceptions

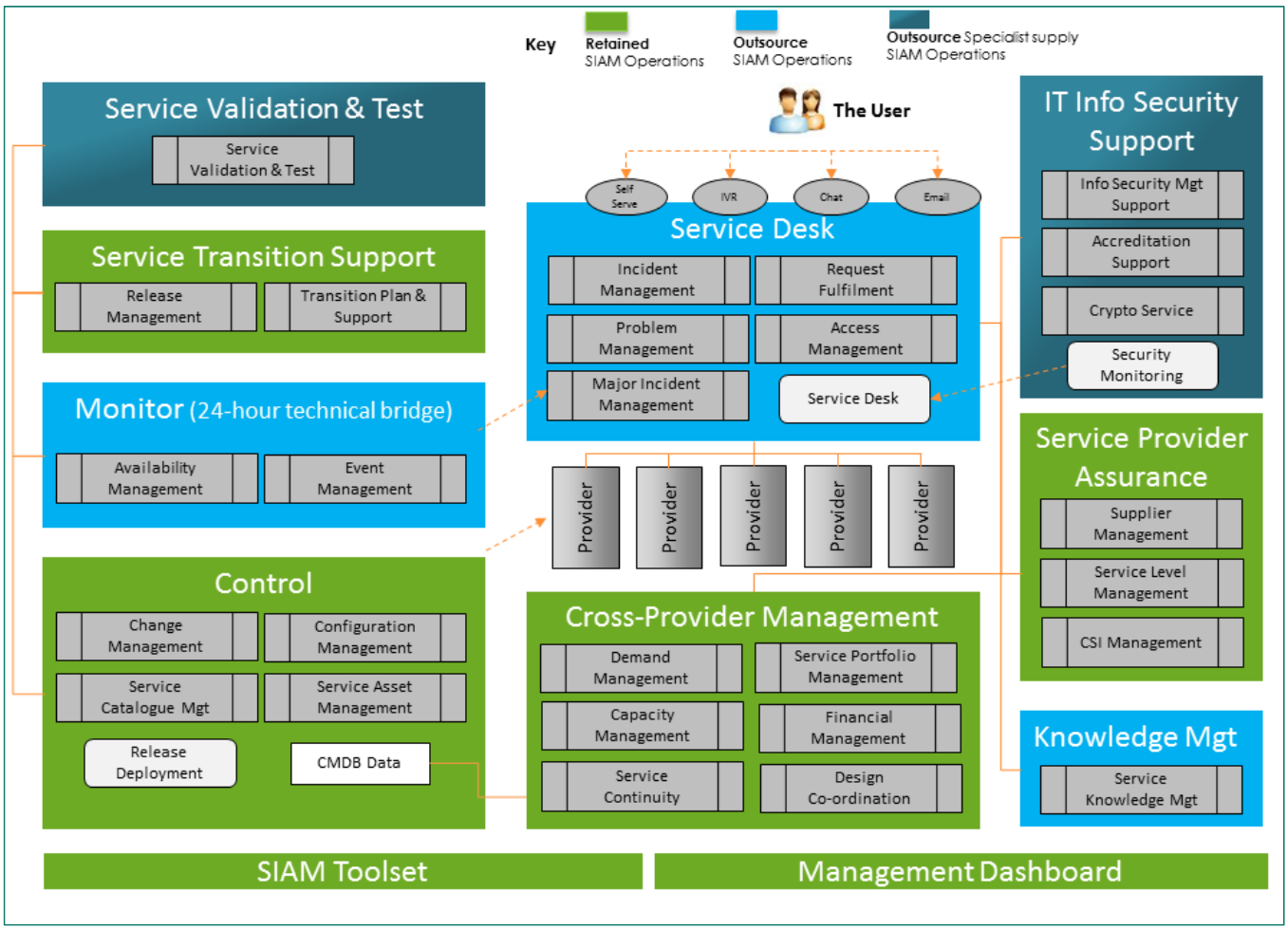
Any requests for exceptions to this document must be submitted in writing and will be reviewed on a case-by-case basis. Exceptions shall be permitted only after documented approval from the Head of SIAM or Chief Information Officer.

1.4 Compliance and Monitoring

All SIAM processes will be audited on a periodic basis. This is to ensure that the processes, guidelines and standards set forth in this document and related process documents are adhered to.

2 SIAM TARGET SERVICE OPERATING MODEL

2.1 Diagram



2.2 Functional Groups

2.2.1 Service Desk

The service desk is the single point of contact for end users to log incidents and requests and provides an interface between the business and supporting IT services with the express purpose of restoring service as quickly as possible.

Restoration of service may be provided by:

- Access to appropriate technical assistance.
- Logging of service requests for access to resources and equipment.
- Providing access to the appropriate information and tools that enable the end user to resolve their own query / incident.

These activities are supported by appropriately skilled staff, robust processes and are underpinned by a highly integrated, flexible and proven ITSM toolset. This approach ensures a consistent and reliable customer experience that aims to reduce overall costs by empowering the customer and providing a proactive service with minimal intervention from other IT areas. The service desk solution strives to deliver industry leading first time fix rates through our integrated processes, tools and appropriately skilled staff.

The key service desk processes are:

1. Incident Management
   - Incident Identification
   - Incident Logging
   - Incident Triage
   - Incident Investigation
   - Incident Resolution
   - Incident Closure
   - Incident Monitoring
2. Major Incident Management
   - Major Incident Review and Acceptance
   - Major Incident Investigation and Diagnosis
   - Major Incident Review and Closure
   - Major Incident Monitoring
3. Problem Management
   - Problem Identification
   - Problem Logging
   - Problem Investigation and Diagnosis
   - Problem Closure
   - Problem Review and Reporting
4. Request Fulfilment
   - Service Request Submission
   - Service Request Authorisation
   - Service Request Review
   - Service Request Fulfilment
   - Service Request Closure

5. Access Management
    - Process Access Requests
        - Requesting Access
        - Verification of Access Requests
        - Amending Access Rights
    - Governing Access
        - Conducting Access Reviews
        - Maintaining User Roles and Access Profiles

2.2.2 Knowledge Management

The knowledge management function is responsible for the provision of, and access to, an appropriate store of knowledge and information artefacts relating to the provision, support and maintenance of IT services. It enables the provision of quality IT services and contributes to the provision of quality end-to-end services by ensuring that those responsible for managing the IT services and end–to-end services are able to do so with access to all current, relevant and appropriate information. The purpose of knowledge management is to ensure that the right person has the right knowledge at the right time to deliver and support the IT services provided.

The only process included within this function is:

1. Knowledge Management
    - Knowledge Creation
    - Periodic Knowledge Article Review and Updates
    - Knowledge Assurance and Maintenance

2.2.3 Monitor

The monitor function is the aggregation point for supporting technologies and provides specific resources and tools for the effective monitoring of the services under management. The monitor function also provides support and management for the Security Operations Centre (SOC) and the capability for the ITSM toolset to receive information from operational tooling. By aggregating via a single point, consistency can be driven into monitoring standards across the estate and dashboards can be presented in a consistent format.

The processes that are included within this function are:

1. Availability Management
    - Definition of Availability Plan
    - Availability Risk Assessment
    - Implementation of Availability Counter-Measures
    - Testing of Availability Measures
    - Definition of Planned IT Maintenance
    - Availability Monitoring
2. Event Management
    - Event Definition
    - Event Detection and Triage
    - Event Investigation
    - Event Review
    - Event Closure

2.2.4 Control

The control function ensures the stability, integrity and availability of live service. Control ensures that all proposed changes to the production environment are managed, planned and communicated and that any releases are communicated and assessed by all suppliers and the customer. It ensures that all underpinning information, in the form of service information down to configuration items (CIs), remains current and aligned to the business requirements.

This also applies to federated instances of information, where it is the responsibility of individual service providers to manage content within the overall structure, as defined by SIAM control.

The processes that are included within this function are:

1. Change Management
    - Change / RFC Creation
    - Change Review and Assessment
    - Change Authorisation
    - Change Implementation
    - Change Closure
2. Configuration Management
    - Configuration Item Planning and Identification
    - Configuration Item Control
    - Status Accounting and Reporting
    - Verification and Audit
    - Asset Management
3. Service Catalogue Management
    - Regular Service Catalogue Review and Change Request Handling
    - Service Catalogue Content Maintenance
    - Service Catalogue Content Activation

2.2.5 Cross-Provider Management

The cross-provider management function ensures that the business maintains a clear view and influence into the cross-delivery services. It also ensures that service operations remains aligned to strategic management decisions by providing service portfolio, demand and financial management. For example, the critical elements of demand management and financial management monitor the ebb and flow of demand and consumption across service providers and provide management information that is critical to resourcing, prioritisation and management of new services being considered via the service portfolio management pipeline. Also, by having these strategic management processes within the scope of service integration, there is a greater ability to understand the full scope of services throughout the service lifecycle across the service providers. IT service continuity management provides the organisation with a surety of service by ensuring that the service provider's service continuity plans are integrated in an end-to-end fashion and that there is alignment to the organisation's service continuity plans and requirements.

The processes included within this function are:

1. Demand Management
    - Create Pattern of Business Activity / User Profile
    - Create Demand Plan
    - Manage Planned Activity
    - Monitor Consumption
2. Capacity Management
    - Create, Update and Review Annual Business Capacity Plan
    - Create, Update and Review Annual Service Capacity Plan
    - Identify and Agree Capacity Optimisation
    - Implement and Validate Adjustments to Service Capacity
    - Monitor Service Capacity Thresholds
    - Capacity Reporting
3. IT Service Continuity Management
    - Requirements and Strategy
    - Implementation
    - On-going Operation
    - Invocation

4. Service Portfolio Management
   - Initiate
   - Define
   - Analyse
   - Approve
   - Review Portfolio
5. Finance Management
   - Definition of Cost Models
   - Raise Purchase Order
   - Invoice Validation
   - Recharge
6. Service Design Coordination
   - Create Design Plan
   - Produce Service Design Package
   - Monitor Design Process

2.2.6 Service Provider Assurance

The service provider assurance function takes responsibility for the delivery of the organisational structures and processes needed to deliver high-quality services across the supply chain. This service aims to deliver the culture and value alignment and the development of a common purpose, attitudes and behaviours across all service providers to drive success for the business.

Using an independent party to perform these activities often allows the customer to focus on strategic issues (and escalations) whilst the detailed tactical discussions and day-to-day issues are dealt with on their behalf. Where this is delivered by an independent party they are able to facilitate discussions and negotiations acting in a more impartial role than either the client or service provider could.

The processes included within service provider assurance are:

1. Continual Service Improvement
   - Receive, Identify and Prioritise CSI Opportunities
   - Define and Implement Service Improvement
   - Measure and Analyse Results
   - Communicate Service Improvement
2. Service Level Management
   - Required Service Level Determination
   - SLA Documentation, Negotiation and Agreement
   - Performance Reporting and Analysis
   - Performance Credit Calculation

2.2.7 Service Transition Support

Service transition support is responsible for the co-ordination of resources and provision of a common re-usable transition framework that supports a comprehensive set of plans to support and execute effective change. This is achieved through the use of consistent and repeatable process and activities that evaluate IT service capability and risk before a new or changed IT service is deployed through release management.

The processes included within this function are:

1. Release Management
   - Define Release Plan
   - Build and Test Release
   - Release Readiness / Deployment
   - Early Life Support
   - Release Review and Closure
2. Transition Planning and Support
   - High-Level Service Transition Planning
   - Low-Level Service Transition Planning
   - Managing Transition

2.2.8 Service Validation and Test

The service validation and test function is responsible for defining a number of key principles to ensure that testing representatives internally and across all service providers are engaged early in the lifecycle, have sufficient independence and operate in a repeatable and measurable manner to well-defined products, processes and controls. Service validation and test can be applied at any point throughout the service lifecycle to quality assure any aspect of a service, capability, resources and capacity to deliver a service and/or service release successfully.

Service validation and test identifies potential risks associated with the implementation of a new or changed service, manages risk mitigation and ultimately improves confidence that a new or changed service will deliver the value and outcomes required. To ensure an end-to-end approach across suppliers and services, an overarching test strategy is defined with which all service providers must comply and ensure compliance and alignment of their own test strategies and plans.

The only process included within this function is:

1. Service Validation and Test
   - Plan, Design and Verify Service Test Plans
   - Execute Service Testing
   - Operational Acceptance Testing
   - Service Management Acceptance Testing
   - Validate Test Reports and Exit Criteria
   - Test Closure

2.2.9 IT Information Security Support

The IT information security support function develops, implements and maintains a cross-provider information security management service (including physical and logical security administration processes) to ensure that the IT services meet all applicable security requirements, including client and service providers information security policies, contractual requirements, legislative and statutory requirements and performance as expressed in the service levels (subject to approval by client management).

The processes included within this function are:

1. Information Security Management Support
   - Security Design and Build
   - Security Monitor and Review
   - Handling Security Incidents and Support
2. Accreditation Support
   - Initial Assessment
   - Planning and Documentation
   - Review and Accredit
   - On-Going Monitoring
3. Crypto Service
   - Design and Creation
   - Deployment and Archiving
   - Monitoring and Audit

3 ORGANISATIONAL BOUNDARIES OF RESPONSIBILITY

3.1 Service Integrator

The role of the service integrator is to own and define the SIAM processes and supporting tools. The service integrator provides governance over the service providers' service management processes and tools to achieve alignment with the over-arching SIAM process and tools. The service integrator will track and monitor the completion of the processes (e.g. the closure of an incident) throughout the lifecycle. They will report on general performance of the SIAM processes including adherence to process by all parties and achievement of the critical success factors for the processes. The service integrator will ensure that reporting and trend analysis supports continual service improvement across all processes to ensure that trends are identified, lessons are learned and appropriate actions are taken. The service integrator will be responsible for customer satisfaction both as a stand alone activity and in terms of managing delivery against agreed SLAs, handling non-delivery against SLAs and managing customer escalations or complaints.

Many organisations wish to procure a service desk separately; some for historic reasons and others where they wish to perform the service integration role internally while sourcing only the service desk. Where the service desk is separated from the service integrator organisation, the service integrator supports the service desk in the delivery of the service desk processes. The service integrator will define the processes, to ensure the service desk processes are optimised and integrated with all other SIAM processes and provide a point of escalation to the service desk provider.

If the service desk function is provided by the service integrator, the service integrator provides the call handling and first time fix capabilities required to support the service desk processes, as listed under the service desk functional group in the previous section.

3.2 Organisation

The organisation shall specify the requirements for each of the SIAM processes. The organisation will own the standards and policies for the processes. The organisation will own the contracts with the service providers and act as a point of escalation where there are issues with the delivery of a service provider. The organisation is both responsible and accountable for the procurement of services in a manner which supports the integration of services, ensuring that service contracts offer unambiguous boundaries of service responsibility and include the necessary integration responsibilities to make the SIAM successful in their role. The organisation will receive reports from the service integrator and will make decisions around actions to be taken and provide the relevant funding, where necessary.

3.3 Service Provider

The service providers shall manage and oversee the SIAM processes across the services / 3rd party suppliers under their management. The service provider will collaborate with the service desk, service integrator and other service providers to manage the cross-delivery processes. This group will provide 2nd tier troubleshooting, monitoring, coordination and escalation function for the 3rd party suppliers they manage / support. A chain of 3rd party suppliers may support some services and these will be managed end-to-end by the service provider.

4 PROCESS RESPONSIBILITIES IN SIAM ENVIRONMENT

Process		Organisation	Service Integrator	Service Provider
Service Desk	Incident Management			
	Major Incident Management			
	Problem Management			
	Request Fulfilment			
	Access Management			
Knowledge Management	Knowledge Management			
Monitor	Availability Management			
	Event Management			
Control	Change Management			
	Configuration Management			
	Hardware Asset Management			
	Software Asset Management			
	Service Catalogue Management			
Cross-Provider Management	Demand Management			
	Capacity Management			
	IT Service Continuity Management			
	Service Portfolio Management			
	Financial Management			
	Service Design Coordination			
Service Provider Assurance	Continual Service Improvement			
	Service Level Management			
	Supplier Management			
Service Transition Support	Release Management			
	Transition Planning and Support			
Service Validation and Test	Service Validation and Test			
IT Information Security Support	Information Security Management Support			
	Accreditation Support			
	Crypto Service			

5 SERVICE DESK PROCESS STATEMENTS

5.1 Incident Management Process

Incident management is defined by ITIL as: “The process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimised.”

This statement supports the Incident Management Process and covers all mandatory activities of the three main parties involved in the process.

For this process, the service provider is split into service desk and operations (resolver groups).

5.1.1 Organisation

The organisation shall:

- Define, make available and maintain the incident management process and policy.
- Communicate the incident management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the incident management policy results in a formal review, which may result in disciplinary action.
- Ensure all appropriate checks have been made prior to reporting an incident to the service desk.
- Ensure all relevant and required details are provided to the service desk when reporting incidents.
- Raise incidents with the service desk when experiencing service disruption or when it becomes aware of a service failure.
- Provide information to the service desk on the business impact of incidents and failures.
- Confirm fault resolution and service restoration within the required timescales to the service desk.
- Where appropriate, perform incident management in accordance with the incident management policies and procedures.
- Make all reasonable attempts to comply with requests made by the service desk or service provider to undertake simple on-site tasks or provide information to effect the resolution of the incident.
- Make every effort to provide incident resolution confirmation.

5.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved organisation policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to the organisation and service providers in fulfilling their incident management roles and responsibilities.
- Where required as a service provider, perform incident management in accordance with the incident management process, policy and procedures.
- Continuously monitor on-going incident resolution.
- Continuously monitor service provider collaboration.
- Organise and conduct service integration meetings if there are issues between various service providers that need to be handled.

5.1.3 Service Provider (Service Desk)

The service desk shall:

- Accept contacts and reports of technical faults and failures from service providers and suppliers.
- Accept and record all incidents reported by users.
- Ensure that all incidents and faults reported are recorded in the service management system.
- Validate, categorise and prioritise all reported incidents and allocate incident severity levels for all incidents and faults reported to the service desk.
- Apply first line fix if possible.
- Assign correctly reported incidents to the appropriate service provider resolver group.
- Provide incident updates to users when requested.
- Accept all resolved incidents received from service provider resolver groups where full resolution and closure details have been provided by the service provider or return back to the service provider any incidents that do not have closure details.
- Close all incidents once the incident resolution has been confirmed.
- Inform the user who reported the incident that the incident has been closed.
- Create a problem record to investigate the root cause if the incident has occurred several times.
- Actively participate in the service integration meeting providing options for issue resolution.

5.1.4 Service Provider (Operations)

The service provider (operations) shall:

- Adhere to the defined and approved ORGANISATION policy and process.
- Provide details of their support organisation and contact points to the service integrator to enable accurate assignment of incidents by the service desk.
- Inform the service desk when they become aware of a fault or failure and indicate the impact to the organisation.
- Accept and acknowledge incidents that are correctly assigned by the service desk.
- Return incorrectly assigned incidents to the service desk.
- Log all IT-related incidents on the service management system.
- Allocate incident severities in accordance with the incident severity definitions contained in the incident management policies and procedures.
- Raise RFCs , where required, to ensure fixes are applied in-line with the Change Management Process.
- Provide updates on the progress of incidents when requested to do so by the service desk.
- Resolve incidents, where relevant, and inform the service desk of incident resolution.
- Actively participate in the service integration meeting providing options for issue resolution.

5.2 Major Incident Management Process

Major incidents are defined by ITIL as: “The highest category of impact for an incident. A major incident results in significant disruption to the business.”

This statement supports the Major Incident Management Process and covers all mandatory activities of the three main parties involved in the process.

5.2.1 Organisation

The organisation shall:

- Define, make available and maintain the major incident management process and policy.
- Communicate the major incident management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the major incident management policy results in a formal review, which may result in disciplinary action.
- Allocate appropriate organisation representatives to be part of the major incident management team.
- Support major incident meetings where required.
- Support the production of the communicatons plan.
- Ensure all changes that support the resolution of a major incident and require a specific service, application, system outage or invocation of IT Service Continuity Management process and procedures have been agreed with the respective business owners.
- Confirm when the solution has been applied and the service restored.
- Participate in any major incident reviews.

5.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Review and validate incidents and accept as major incidents.
- Assign incidents to a major incident manager.
- Lead and manage the major incident resolution forum with the organisation and appropriate service providers for all severity 1 (major) incidents.
- Perform a critical incident assessment and make the final decision on whether BCP / DR is to be invoked.
- Monitor all on-going major incident resolution activities and service provider collaboration.
- Verify incident resolution.
- Lead any major incident review meetings.
- Review and publish major incident reports to all relevant stakeholders.
- Identify service improvements based on input from service providers and organisation.
- Conduct service integration meetings to resolve issues between service providers, ensuring fair and productive feedback.

5.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide a major incident manager to manage the incident resolution and pull together the MIM team.
- Support major incident meetings where required.
- Produce all relevant communications plans.
- Investigate and diagnose the major incident and call on other service provider assistance as required.
- Produce action plan and service resoration plan.
- Apply permanent fix or workaround, monitor the service for an agreed time and report findings.
- Document the applied solution and ensure incident record is kept up-to-date.
- Participate in major incident reviews and create the major incident report.
- Actively participate in service integration meetings, providing options for issue resolution.

5.3 Problem Management Process

Problem management is defined by ITIL as: “The process responsible for managing the lifecycle of all problems. Problem management proactively prevents incidents from happening and minimises the impact of incidents that cannot be prevented.”

This statement supports the Problem Management Process and covers all mandatory activities of the three main parties involved in the process.

For this process, the service provider is split into service desk and operations (resolver groups).

5.3.1 Organisation

The organisation shall:

- Define, make available and maintain the problem management process and policy.
- Communicate the problem management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the problem management policy results in a formal review, which may result in disciplinary action.
- Provide up-to-date business impact information to enable the service provider to provide accurate prioritisation of problems.
- Participate in the evaluation of any solutions proposed by the service provider to resolve problem.

5.3.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to the organisation and service providers in fulfilling their problem management roles and responsibilities.
- Confirm priority of significant problems.
- Formally sign-off all solution approvals and approve workarounds when required.
- Continuously monitor on-going problem resolution.

- Continuously monitor service provider collaboration.
- Organise and conduct periodic problem review meetings.
- Produce and distribute any relevant management reports and minutes from the problem review meeting.

5.3.3 Service Provider (Service Desk)

The service desk shall:

- Log problems in accordance with the problem management process, policy and procedures.
- Initiate problem reviews based on trend analysis.
- Identify, prioritise, assist and manage through to resolution those problems that cause, or have the potential to cause, business disruption.
- Investigate problem records and link to any known errors / workarounds, if available.
- Assign problems to the appropriate service provider resolver groups.
- Coordinate problem management activities which span multiple service providers.
- Receive problems for external assignment from service providers and assign them to the appropriate service provider.
- Ensure service providers conduct root cause analysis on any problems raised and that the problem record is updated accordingly to reflect the analysis.
- Ensure problem records are maintained, kept up-to-date and closed when resolved.
- Proactively monitor problem volumes.
- Collate, maintain and publish accurate and up-to-date information on problems, workarounds and known errors to the organisation.
- Monitor and report to the organisation overall business impact and the effectiveness of workarounds proposed by service providers.
- Regularly review problems ensuring incidents are accurately linked and use this information to proactively review and revise problem severities where necessary.
- Identify potential process improvements and make appropriate recommendations to service providers and the organisation.
- Actively participate in the periodic problem review meetings providing options for issue resolution and prevention of problems re-occurring.

5.3.4 Service Provider (Operations)

The service provider (operations) shall:

- Adhere to the defined and approved policy and process.
- Identify potential problems and raise with the service desk.
- Initiate problem reviews based on trend analysis.
- Submit fully-documented and validated problem records to the service desk using the standard problem template.
- Accept and resolve problems when they are correctly assigned to the service provider.
- Acknowledge correctly assigned problems within the required timescales.
- Inform service desk of any problems that have been incorrectly assigned to them.
- Provide progress updates on problems in a timely manner to service desk through the problem lifecycle.
- Perform root cause analysis on problems including developing corrective actions and/or workarounds for all problems.
- Provide diagnostic scripts and other problem determination aids to service desk to prevent repetitive issues.
- Implement relevant workarounds / problem resolutions.
- Ensure problem records are kept up-to-date and close records once resolutions have been applied.
- Continually evaluate the linked incident count to known errors and problems to ensure the business impact is current.
- Actively participate in the periodic problem review meetings providing options for issue resolution and prevention of problems re-occurring.

5.4 Request Fulfilment Process

Request fulfilment is defined by ITIL as: “The process responsible for managing the lifecycle of all service requests.”

This statement supports the Request Fulfilment Process and covers all mandatory activities of the three main parties involved in the process.

5.4.1 Organisation

The organisation shall:

- Define, make available and maintain the request fulfilment process and policy.
- Communicate the request fulfilment policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the request fulfilment policy results in a formal review, which may result in disciplinary action.
- Ensure all relevant and required details are provided to the service desk when submitting service requests.
- Ensure that all requests have the appropriate level of approval.
- Provide confirmation to the service desk that the service request has been fulfilled.

5.4.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to the organisation and service providers in fulfilling their service request management roles and responsibilities.
- Arrange, manage and lead the service request management operational review meeting.
- Review service provider management information on a monthly basis and produce trend analysis and management summaries to identify trends or significant changes or increases in service request

volumes, for discussion with the organisation and the service providers.
- Identify potential process improvements and make appropriate recommendations to the organisation and service providers.
- Monitor and manage stakeholder compliance to the request fulfilment process, policy and procedures.
- Inform service providers of any service provider material non-compliance with the request fulfilment process, policy and procedures.
- Engage with service desk, service providers and organisation where there are issues and problems with the processing of service requests.
- Ensure that service requests are expedited within agreed timescales by service providers when assigned by the service desk.
- Ensure that all relevant information is provided by service providers in response to service requests.
- Accept and record all service requests submitted by users.
- Ensure that all service requests submitted are recorded in the service management system.

5.4.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide details of their support organisation and contact points to the service integrator to enable the accurate assignment of service requests by the service desk.
- Accept and acknowledge service requests that are correctly assigned by the service management tool.
- Return incorrectly assigned service requests to the service desk.
- Provide updates on the progress of service requests when requested to do so by the service desk.
- Inform the service desk when a service request has been completed.
- Provide management information, in each service management period, to the appropriate service request forums.

5.5 Access Management Process

Access management is defined by ITIL as: “The process responsible for allowing users to make use of IT services, data or other assets. Access management helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorised users are able to access or modify them. Access management implements the policies of information security management and is sometimes referred to as rights management or identity management.”

This statement supports the Access Management Process and covers all mandatory activities of the three main parties involved in the process.

5.5.1 Organisation

The organisation shall:

- Define, make available and maintain the access management process and policy.
- Communicate the access management policy and process to service integrator and service providers.
- Ensure that non-adherence to the access management policy results in a formal review, which may result in disciplinary action.
- Issue requests for user access to the service integrator using the required format or tool.
- Define and ensure the appropriate approval process is in place and followed by users when requests are being made.
- Compare the system extract provided by the service provider with the list of approved users in the business unit, identify any exceptions and inform the service integrator of the outcome.
- Implement concepts of user and group access types to ensure access is granted in a regulated manner.
- Enforce directory services and group policy objects standards across all service providers and services.

5.5.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Initiate scheduled access reviews (based on a pre-defined periodic schedule).
- Request a system list / extract of users with access to the system from the service provider.
- Review feedback from organisation on exceptions, upload all relevant information in the SKMS and raise an incident to investigate.
- Inform the Service Provider to revoke user access, where required.
- Review confirmation of access revocation and all relevant supporting documentation / evidence and approve completion.
- Enforce directory services and group policy objects standards across all service providers and services.
- Schedule periodic audits to ensure correct user access has been provided to systems.
- Inform the organisation where it suspects inappropriate user access has been requested.

5.5.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Inform the service integrator where it suspects inappropriate user access has been granted (e.g. where the service provider believes that inappropriate access has been granted during the investigation of an incident).
- Extract the list of users with access to the system (when requested by the service integrator), ensure this list is tamper-proof and forward to the organisation for review.
- Revoke any access requested by service integrator, fix issues and confirm once done.
- Enforce directory services and group policy objects standards across all service providers and services.
- Maintain and manage user roles, profiles and group policy objects.

6 KNOWLEDGE MANAGEMENT PROCESS STATEMENTS

6.1 Knowledge Management Process

Knowledge management is defined by ITIL as: “The process responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time. The knowledge management process enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge.”

This statement supports the Knowledge Management Process and covers all mandatory activities of the three main parties involved in the process.

6.1.1 Organisation

The organisation shall:

- Define, make available and maintain the knowledge management process and policy.
- Communicate the knowledge management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the knowledge management policy results in a formal review, which may result in disciplinary action.
- Ensure that all relevant business information is made available to the service integrator to enable the development of the service knowledge management system (SKMS).
- Ensure that knowledge articles under their ownership are kept accurate, up-to-date and are reviewed on a periodic basis.

6.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Define and maintain the knowledge management strategy.
- Establish and maintain knowledge management interfaces and transfer mechanisms.
- Establish and maintain data requirements.
- Establish data and information management procedures.
- Develop the service knowledge management system.
- Ensure service knowledge management information is accessible and available to all interested parties.
- Capture, store, analyse and share data effectively across lifecycle processes and service providers.
- Evaluate all knowledge articles to ensure they are of sufficient quality.
- Initiate SKMS audit to assure that knowledge articles are accurate and up-to-date, no knowledge articles are missing and obsolete knowledge articles are discarded.
- Ensure that knowledge articles are updated, added or discarded where appropriate.

6.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Ensure that all relevant service provider information is made available to the service integrator to enable the development of the SKMS.
- Ensure that knowledge articles under their ownership are kept accurate, up-to-date and are reviewed on a periodic basis.

7 MONITOR PROCESS STATEMENTS

7.1 Availability Management Process

Availability management is defined by ITIL as: “The process responsible for ensuring that IT services meet the current and future availability needs of the business in a cost-effective and timely manner. Availability management defines, analyses, plans, measures and improves all aspects of the availability of IT services, and ensures that all IT infrastructures, processes, tools, roles etc. are appropriate for the agreed service level targets for availability.”

This statement supports the Availability Management Process and covers all mandatory activities of the three main parties involved in the process.

7.1.1 Organisation

The organisation shall:

- Define, make available and maintain the availability management process and policy.
- Communicate the availability management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the availability management policy results in a formal review, which may result in disciplinary action.
- Provide business requirements to the service integrator, where required.
- Review and approve availability requirements provided by the service integrator.
- Contribute to the review and approval of the availability plan produced by the service integrator.
- Carry out service failure analysis with the service integrator and propose counter-measures.
- Review documented remediation actions provided by the service integrator and approve expenditure or accept risks.
- Provide input to the definition and agreement of IT maintenance windows.

7.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to service providers in fulfilling their availability management roles and responsibilities.
- Develop, maintain, review and distribute the availability plan in accordance with the availability management process, policy and procedures.
- Co-ordinate any proposed improvement activities that span multiple service providers.
- Identify and inform the service providers of the end-to-end measurement elements that need to be measured in the reporting against the end-to-end service availability targets.
- Define scope of risk assessment, initiate and request service failure impact analysis from organisation and service provider.
- Receive the reports from organisation and service provider and consolidate into a single end-to-end failure impact report, including all proposed counter-measures.
- Define risk-mitigating and cost-justifiable counter-measuresand and create and publish availability risk report.
- Agree or reject risk-mitigating counter-measures and/or remediation actions proposed by the service providers.
- Review implementation of counter-measures and remediation actions in order to ensure that counter-measures are effective in meeting availability service levels and are sufficiently mitigating risks associated with unavailability.
- Ensure alignment of disaster recovery plans with the implemented counter-measures and/or remediation actions.
- Initiate testing of counter-measures / remediation actions.
- Review availability test strategy and plan provided by the service provider.
- Evaluate test results and define cost-justifiable initiatives and forward proposal to organisation.
- Provide input to the definition and agreement of IT maintenance windows.
- Create and release the integrated IT maintenance plan.
- Continuously monitor on-going availability management.
- Continuously monitor service provider collaboration.
- Organise and moderate service integration meeting.
- Monitor, analyse and calculate the performance of service providers against the end-to-end KPIs, consolidate and report to the organisation.
- Provide a consolidated report to the organisation for the measurement of the defined organisation critical business transactions.
- Review the end-to-end KPIs with the organisation and document and communicate any areas for improvement to the service providers.

7.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of the availability management procedures and supporting documentation.
- Assist the service integrator in the creation of the end-to-end pictorial component and application overview to enable the development and on-going maintenance of the availability plan.
- Review and provide input to the availability plan provided by the service integrator.
- Evaluate the effectiveness of their own availability management process and implement changes to improve efficiency.
- Work with the service integrator and other service providers to assist with any service provider engagement and non-compliance issues.
- Undertake component failure impact analysis (CFIA) and single points of failure (SPOF) analysis.

- Design and implement counter-measures / remediation actions.
- Coordinate the business and service integration resources to participate in testing activities and document the test activities, results and proposed improvements in an availability test report.
- Provide input to the definition and agreement of IT maintenance windows.
- Actively participate in the service integration meeting, providing options for issue resolution.
- Execute agreed corrective actions.

7.2 Event Management Process

Event management is defined by ITIL as: “The process responsible for managing events throughout their lifecycle. Event management is one of the main activities of IT operations.”

This statement supports the Event Management Process and covers all mandatory activities of the three main parties involved in the process.

7.2.1 Organisation

The organisation shall:

- Define, make available and maintain the event management process and policy.
- Communicate the event management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the event management policy results in a formal review, which may result in disciplinary action.
- Assist service providers and the service integrator in the investigation of events.

7.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Identify all service components to be monitored with the relevant service provider.
- Define an escalation path for each event with the relevant service providers and approve if it meets business needs
- Initiate the implementation of the event design.
- Approve or reject refined event thresholds.
- Log, consolidate and analyse activity on agreed devices on the organisation's estate and at the perimeter to identify in real-time any anomaly that might constitute an event.
- Ensure events identified as potential incidents are adequately investigated by the relevant service provider and recorded and tracked as an incident.
- Ensure that in all cases where a service risk is identified, the service providers take remedial action as necessary and agreed with the organisation - including, where appropriate, coordinating the activities of the service providers involved.
- Receive and record all events and incidents.

7.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Notify the service integrator when it becomes aware of an event and provide all necessary details and information of such event.
- For new or changed services:
  - Identify event options
  - Select event types
  - Define event thresholds
  - Define event correlation conditions
  - Define alert content
  - Define event escalation
  - Forward overall design to service integrator for approval.
- Investigate, contain, track, manage and resolve events.
- Refine event thresholds.
- Configure and re-tune monitoring tools.
- Ensure event documentation is kept up-to-date.

8 CONTROL PROCESS STATEMENTS

8.1 Change Management Process

Change management is defined by ITIL as: “The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.”

This statement supports the Change Management Process and covers all mandatory activities of the three main parties involved in the process.

8.1.1 Organisation

The organisation shall:

- Define, make available and maintain the change management process and policy.
- Communicate the change management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the change management policy results in a formal review, which may result in disciplinary action.
- Provide impact assessments of requests for change (RFCs) where required.
- Provide relevant / suitable attendees at the change advisory board (CAB).
- Provide relevant / suitable attendees at the post-implementation review (PIR).

8.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to service providers in fulfilling their change management roles and responsibilities.
- Schedule the implementation of change requests.
- Identify, manage and co-ordinate change requests that require involvement and activity by multiple service providers with the objective of achieving the successful implementation of the overall change request.
- Undertake appropriate activities to enable the maximisation of service availability by minimising the business disruption caused by change activities.
- Arrange and manage CAB meetings and emergency CAB meetings.
- Ensure that any issues raised at the CAB are progressed satisfactorily.
- Ensure RFCs are updated throughout their lifecycle and in-line with the decisions made at the CAB.
- Ensure that post implementation reviews (PIRs) are held and managed effectively when required.
- Develop, manage, maintain and communicate to stakeholders the forward schedule of change.
- Review service provider management information and produce trend analysis and management summaries to identify change volumes and trends for discussion with the department and the service providers at the appropriate forums.
- Identify potential process improvements, make appropriate recommendations and manage through any process improvement activity.
- Monitor and manage service providers’ compliance with the change management process, policy and procedures and report any non-compliance.

8.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of the change management procedures and supporting documentation.
- Log and track changes during their lifecycle.
- Ensure that RFCs submitted are completed.
- Ensure that any RFC raised has sufficient justification and are submitted in sufficient time to avoid the need for the service integrator to initiate urgent action to ensure the change is implemented to the required timescale.
- Ensure the RFC is updated during its lifecycle.
- Ensure that impacts are returned within the required timescale and that the correct information is included to aid the progression of the change request.
- Ensure that changes raised are scheduled during a scheduled maintenance window.
- Ensure the change owner brokers positive impact assessment and endeavours to resolve negative impacts.
- Ensure that any cancelled RFC identifies the reasons for the cancellation.
- Provide input to CAB by:
  - Providing suitably empowered representation.
  - Ensuring all management summaries are submitted by the required date and time and meet the required entry criteria.
  - Ensure that notification of the approval decision is disseminated as appropriate within its own organisation.
  - Ensuring that if it conducts internal governance or assurance of release and test proposals or release collateral, that it gathers such evidence ahead of CAB.
- Ensure that a PIR is completed and any actions arising are progressed accordingly.
- Ensure that the outcome of any implementation activity is detailed on the RFC.
- Monitor, analyse and report to the service integrator on change volumes and trends.
- Implement any resulting improvement activity.
- Work with the service integrator and other service providers to assist with any service provider engagement and non-compliance issues.

8.2 Service Asset and Configuration Management Process

Service asset and configuration management is defined by ITIL as: “The process responsible for ensuring that the

assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets."

This statement supports the Configuration Management Process, Hardware Asset Management Process and Software Asset Management Operating Model and covers all mandatory activities of the three main parties involved in the processes.

8.2.1 Organisation

The organisation shall:

- Define, make available and maintain the service asset and configuration management policy and processes.
- Communicate the service asset and configuration management policy and processes to the service integrator and the service providers.
- Ensure that non-adherence to the service asset and configuration management policy results in a formal review, which may result in disciplinary action.
- Participate in determining the level of CI granularity and relationships with the service integrator.
- Participate in meetings to determine the levels of service asset and configuration management integration required between the service integrator and service provider.

8.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the processes.
- Provide support and guidance to service providers in fulfilling their service asset and configuration management roles and responsibilities.
- Arrange and manage service asset and configuration management service review meetings
- Work with the service provider as reasonably requested with the scoping of audits, impact assessments, investigation and resolution of discrepancies.
- Produce an audit scope document for every approved audit.
- Provide evidence of proactive configuration management by providing the findings of trend analysis activities to the organisation.
- Identify potential process improvements and make appropriate recommendations.
- Monitor and manage stakeholder compliance to the service asset and configuration management policies and procedures and inform service providers of any material non-compliance.
- Liaise with service providers and the organisation, as required, to define and agree the CMDB structure / tooling.
- Ensure any changes to the CMDB structure are processed through the appropriate channel.
- Where required, amend the service provider interface definition documentation via the appropriate process.
- Inform service providers of any CI validation errors found when entering their CI data on the integrated CMDB.
- Regularly provide a detailed sample of recent CI updates made to the integrated CMDB to service providers.
- Report high criticality discrepancies to the service providers and liaise with the service provider to determine actions required to resolve the discrepancy.
- Update the discrepancy reports once all agreed actions have been completed.
- Determine the service asset and configuration management requirements of other service management processes.
- Agree the level of CI granularity and relationships with the service provider, create appropriate CIs and broker them to service providers.
- Process the CI data provided by the service providers and monitor compliance to the service asset and configuration management processes, policy and procedures post project go-live.
- Implement and manage a single enterprise asset management service.
- Ensure that all service providers record all attributes of an asset so that it can be accurately determined.
- Ensure that end of life and retired assets are removed from active use and are made available for re-use where appropriate.

8.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of the relevant procedures and supporting documentation to support the delivery of the processes.
- Work with the service integrator and the organisation as reasonably required with the scoping of audits, impact assessments, investigation and resolution of discrepancies.
- Provide the required audit data to the service integrator within the required timescales and in the format specified by the service integrator.
- Review and comment on audit scope documents.
- Monitor, analyse and report to the service integrator on the accuracy of the service provider's CMDB and provide evidence of proactive configuration management to the service integrator at the service asset and configuration management service review meetings.
- Work with the service integrator and other service providers to assist with any service provider engagement and non-compliance issues.
- Provide agreed configuration management measurements to the service integrator.
- Develop, test and implement changes to their interfaces and CI data content as defined in the interface definition documentation provided by the service integrator.
- Provide CI data in accordance with the interface requirements of the integrated CMDB.
- Ensure that CI updates are processed in accordance with the configuration management and

change management processes, policies and procedures.
- Update their own CMDB within an agreed number of hours of a corresponding change being made in the live or production test estate and provide the CI data to the service integrator within an agreed number of hours of the change being made to the service provider CMDB.
- Provide details of all change reports under which CI data updates were made upon request from the service integrator.
- Assist the service integrator in determining the reason for each discrepancy, its criticality, the responsible party and actions required to address it.
- Review and comment to the service integrator on discrepancy reports.
- Where requested by the service integrator, provide CI data as requested or provide an explanation to the service integrator as to why the data cannot be provided.
- Agree the level of CI granularity and relationships with the service integrator.
- Provide CI data for new / enhanced services at the earliest opportunity following go-live.
- Meet with the other service providers to determine the level of configuration management integration required and ensure configuration management is not being on-boarded in isolation.
- Develop a process (automated or non-automated) for the provision of CI data to the service integrator.
- Provide service integrator with required asset attributes.

8.3 Service Catalogue Management Process

Service catalogue management is defined by ITIL as: “The process responsible for providing and maintaining the service catalogue and for ensuring that it is available to those who are authorised to access it.”

This statement supports the Service Catalogue Management Process and covers all mandatory activities of the three main parties involved in the process.

8.3.1 Organisation

The organisation shall:

- Define, make available and maintain the service catalogue management process and policy.
- Communicate the service catalogue management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the service catalogue management policy results in a formal review, which may result in disciplinary action.
- Provide new / updated business service description and charging information to the service integrator.
- Provide new / updated request fulfilment workflow to the service integrator.
- Review prepared service catalogue items in order to validate the correctness and fit for purpose.
- Confirm that the prepared catalogue change can be activated.

8.3.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Develop, maintain and distribute the service catalogue.
- Provide on-line access to the service catalogue to the organisation.
- Receive, review and validate requests for a service catalogue change and approve / reject.
- Document the required service catalogue model update in detail (in a service catalogue model design document).
- Determine required catalogue content updates.
- On a regular basis, or according the review schedule, review the service catalogue model and service catalogue content to ensure that they are fit for purpose.
- Review and validate business service description, charging information and request fulfilment workflow received from the organisation.
- Review and validate technical service component descriptions received fro the service provider.
- Update the business and technical service descriptions, as required, in order to ensure that they are in a standard format and are fit for purpose.
- Create / update service catalogue item structure.
- Activate service catalogue change, archive the catalogue and communicate changes.
- Update and/or close requests for service catalogue changes.

8.3.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide all relevant information and assistance to the service integrator in the development of the service catalogue.
- Raise requests in the appropriate format to request changes to the service catalogue.
- Provide new / updated technical service component descriptions.

9 CROSS-PROVIDER PROCESS STATEMENTS

9.1 Demand Management Process

Demand management is defined by ITIL as: “The process responsible for understanding, anticipating and influencing customer demand for services. Demand management works with capacity management to ensure that the service provider has sufficient capacity to meet the required demand. At a strategic level, demand management can involve analysis of patterns of business activity and user profiles, while at a tactical level, it can involve the use of differential charging to encourage customers to use IT services at less busy times, or require short-term activities to respond to unexpected demand or the failure of a configuration item.”

This statement supports the Demand Management Process and covers all mandatory activities of the three main parties involved in the processes.

9.1.1 Organisation

The organisation shall:

- Define, make available and maintain the demand management process and policy.
- Communicate the demand management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the demand management policy results in a formal review, which may result in disciplinary action.
- Contribute in the mapping of patterns of consumption activity to business activity.
- Approve patterns of business activity and user profiles.
- Provide and maintain / update business calendars and roadmaps.
- Agree the demand plan produced by the service integrator.
- Participate in demand management review meetings, as required.
- Implement and report on demand control activities.
- Inform the service integrator of any deviations from the existing demand plan.

9.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Collate and analyse all patterns of consumption activity provided by service providers.
- Lead the mapping of patterns of consumption activity to business activity.
- Define and issue patterns of business activity and user profiles.
- Collate and analyse business demand forecast and identify any conflicts / queries to be fed back to the organisation.
- Assess the demand forecast against patterns of business activity and user profiles.
- Define and issue the demand plan.
- Organise and conduct demand management review meetings.
- Monitor and manage activities that control demand requirements.
- Monitor, identify and collate new and changing demand requirements.

9.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Track consumption, analyse data and identify patterns of consumption activity and provide to service integrator.
- Provide input, as required, to definition of patterns of business activity and user profiles.
- Provide input, as required, to assessment of demand forecast against patterns of business activity and user profiles.
- Assign, implement, track and report on demand control activities.
- Monitor, identify and collate new and changing demand requirements and feedback to service integrator.

9.2 Capacity Management Process

Capacity management is defined by ITIL as: “The process responsible for ensuring that the capacity of IT services and the IT infrastructure is able to meet agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity management considers all resources required to deliver an IT service and is concerned with meeting both the current and future capacity and performance needs of the business. Capacity management includes three sub-processes: business capacity management, service capacity management and component capacity management.”

This statement supports the Capacity Management Process and covers all mandatory activities of the three main parties involved in the processes.

9.2.1 Organisation

The organisation shall:

- Define, make available and maintain the capacity management process and policy.
- Communicate the capacity management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the capacity management policy results in a formal review, which may result in disciplinary action.
- Provide insight into the current and future business events and strategy which may impact capacity.
- Provide to the service integrator the quarterly business forecast (QBF) and any other related IT documentation containing forecast business volumes which enable the service provider to accurately forecast future resource units and detail the assumptions made in the narrative of their quarterly capacity plan (QCP).

- Where appropriate ensure that the correct commercial contract is in place and ensure that funding is available to progress the optimisation opportunity.

9.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to the organisation and service providers in fulfilling their capacity management roles and responsibilities.
- Progress all capacity-related issues raised by the organisation with the appropriate service providers.
- Manage any cross-service provider issues that cannot be resolved directly between the service providers.
- Proactively identify capacity management process improvements, make appropriate recommendations and co-ordinate improvement activities that span multiple service providers.
- Monitor and manage stakeholder compliance to the capacity management policy and procedures and inform service providers of any material non-compliance.
- Coordinate capacity planning activities that span multiple service providers ensuring that forecast and actual data is realistic, appropriate and facilitates the identification of remedial action by, and between, service providers.
- Distribute QBF to the service providers ensuring that key changes that need to be reflected in the service provider's QCP and resource unit forecasts are identified accurately.
- Provide assurance to the organisation that QCP narratives and resource unit forecasts are realistic and align with organisation forecasts, IT strategies and reflect known project engagement.
- Review service provider QCPs to ensure that opportunities for capacity optimisation have been included and, where appropriate, challenge the service provider where no, insufficient or poor quality optimisation opportunities have been included.
- Provide a consolidated QCP that demonstrates an understanding between business demand, use of IT-related services and resource unit consumption.
- Use forecasts and actuals to develop and distribute the volume of services actually consumed (VSAC) report.
- Review and undertake trend analysis of service provider capacity management information.
- Ensure that the wider organisation audience is the focus of all service provider comments and resource unit forecasts.
- Develop and maintain a record of priority optimisation opportunities that have been suggested by service providers that includes the status of each suggestion.
- Discuss service provider proposals for optimisation with service providers and the organisation and create an optimisation opportunity analysis report describing the opportunity, proposed benefits, findings and outcome.
- Where optimisation opportunities are approved by the organisation, monitor the service provider's progress against the plans for optimising capacity.
- Analyse service provider MI to provide a report on the holistic view of performance, cost and risk by service to facilitate a total cost of ownership view and identification of opportunities for business behaviour optimisation.

9.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of the relevant procedures and supporting documentation.
- Ensure that appropriate levels of monitoring of resources and system performance are set and that recorded information is kept up-to-date.
- Provide insight into achieved performance focusing on exceptional performance, performance that does not meet expectations and any underlying issues and actions required to resolve those issues.
- Manage capacity-related changes through to a successful conclusion and confirm they have had the required effect on the management of capacity.
- Escalate to the service integrator any cross-service provider issues that cannot be resolved directly between the service providers.
- Work with the service integrator and other service providers to assist with any service provider engagement and non-compliance issues.
- Support any ad hoc audits that are carried out on the capacity management process.
- Monitor, analyse and report to the service integrator on capacity volumes and trends.
- Analyse the QBFs and provide QCPs in the required format to the service integrator.
- Ensure that forecast narratives and data are realistic, consistent and align with departmental business forecasts, IT strategies and reflect known project engagement.
- Ensure the QCP demonstrates an understanding between business demand, use of IT-related services and resource unit consumption.
- Identify opportunities for optimising capacity in QCPs and recommend appropriate action.
- Respond to, and resolve, any queries raised in relation to the QCP.
- Where required, undertake further analysis of the identified optimisation opportunity and produce a plan that incorporates the analysis and benefits and prioritises service provider activity and discuss with the service integrator / organisation as appropriate.
- When approved, produce a plan for implementation of the proposed optimisation opportunity and manage the activities through to a successful conclusion, reporting progress and issues to the service integrator as they occur.
- Where required, provide information to the service integrator to support the optimisation opportunity analysis.

- Comply with any reasonable request by the service integrator to provide relevant data in the required formats and frequency to enable the service integrator to provide and manage the end-to-end capacity management process.
- Provide an effective process for analysing server capacity requirements as a result of a business change provided by the organisation.
- Ensure that the forecast narrative provides sufficient information to enable the organisation to understand the risks and consequences associated with any action / inaction, the timescales until problems will be experienced and recommended mitigation actions to eliminate or minimise impacts, the likely costs associated with remedial options / action and the decisions required by the organisation.

9.3 IT Service Continuity Management Process

IT service continuity management (ITSCM) is defined by ITIL as: "The process responsible for managing risks that could seriously affect IT services. IT service continuity management ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. IT service continuity management supports business continuity management."

This statement supports the IT Service Continuity Management Process and covers all mandatory activities of the three main parties involved in the processes.

9.3.1 Organisation

The organisation shall:

- Define, make available and maintain the ITSCM process and policy.
- Communicate the ITSCM policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the ITSCM policy results in a formal review, which may result in disciplinary action.
- Review and agree the ITSCM strategy.
- Agree the ITSCM test programme with the service integrator.
- Agree the ITSCM test scope.
- Attend stakeholder meetings, as appropriate, and ensure any customer actions are completed.
- Provide business input to ITSCM risk assessment.
- Provide business input to the ITSCM test.
- Provide a decision on whether or not an ITSCM event should be declared.

9.3.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to the organisation and service providers in fulfilling their ITSCM roles and responsibilities.
- Produce the ITSCM strategy, agree this with the organisation and reset the strategy at least annually.
- Manage the ITSCM risk assessment.
- Progress all ITSCM-related issues raised by the organisation with the appropriate service provider.
- Ensure ITSCM awareness activity is conducted both within the service integration team and across the service provider community.
- Monitor and manage stakeholder compliance to the ITSCM policy, process and procedures and report any non-compliance.
- Review service provider ITSCM information and produce trend analysis and management summaries to identify issues and trends for discussion with the organisation and the service providers at the appropriate forums.
- Commission service providers to undertake service threat assessments, where required.
- Develop and agree the ITSCM plan with the organisation and reset the plan at least annually and maintain to ensure its currency.
- Develop and agree the ITSCM test programme with the organisation and reset the ITSCM test programme at least annually and maintain to ensure its currency.
- Review and agree ITSC plans with service providers.
- Engage with change management to ensure secure individual slots for ITSCM testing purposes in-line with the ITSCM test programme.
- Produce and agree with service providers and the organisation the ITSCM test scope and over-arching test plan.
- Direct and manage ITSC test activities.
- Identify and communicate lessons learnt and update ITSCM products as appropriate.
- During both the execution of a ITSCM test plan and the execution of a real ITSCM event:
  - Attend major incident forums.
  - Prepare event options and recommendations for consideration by the organisation.
  - Direct recovery plan activity.
  - Prepare a plan to return to normal operations within an agreed number of days of an ITSCM event being declared.

9.3.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of the ITSCM procedures and supporting documents.
- Conduct ITSC awareness activity within the service provider's ITSC team.
- Work with the service integrator and other service providers to assist with any service provider engagement and non- compliance issues.
- Perform service threat assessments as directed by the service integrator and report the outcome.
- Analyse root cause analysis and incident closure reports and inform the service integrator of the outcome and raise any current and emerging ITSCM risks required.
- Produce the service provider ITSC plan and agree it with the service integrator.
- Analyse new projects or project changes to determine whether sufficient information is provided

in order to enable impact assessment to be undertaken.
- Identify any project or change related ITSC risks and emerging risks and take appropriate action to mitigate.
- Produce and update ITSC products including test recovery plans.
- Provide information to the service integrator to assist in the completion of the ITSC test programme.
- Contribute to the high-level ITSC test plan and produce low-level test plans.
- Analyse the results of test activity and provide input to the test report and the action plan for any remedial activities.
- Complete any actions required, as detailed in the action plan.
- During both the execution of the ITSCM test plan and the execution of a real ITSCM event, the service provider must:
  - Attend major incident forums.
  - Prepare event options and recommendations for consideration by the organisation.
  - Prepare and update recovery plans.
  - Recover systems and services as directed by the service integrator.
  - Contribute to the production of a plan to return to normal operations within an agreed number of days of an ITSCM event being declared.

9.4 Service Portfolio Management Process

Service portfolio management is defined by ITIL as: “The process responsible for managing the service portfolio. Service portfolio management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. Service portfolio management considers services in terms of the business value that they provide.”

This statement supports the Service Portfolio Management Process and covers all mandatory activities of the three main parties involved in the processes.

9.4.1 Organisation

The organisation shall:
- Define, make available and maintain the service portfolio management process and policy.
- Communicate the service portfolio management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the service portfolio management policy results in a formal review, which may result in disciplinary action.
- Review and approve that new or changed service model meets business requirements.
- Provide input into deciding whether to procure new services and updates to service model.
- Participate in reviewing returns on investment for each service to ensure that the ROI remains aligned to business expectations.
- Participate in a review with the service integrator of any services that are no longer aligned to the business and/or IT strategy or if the ROI has changed.

9.4.2 Service Integrator

The service integrator shall:
- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Receive new or changed service requirements, review and make a decision on whether to accept or reject.
- Review and agree the timelines in which the new / changed service needs to be delivered.
- Disaggregate service requirements into component services and map against the standard service model to identify existing services that may fulfil new requirements and where gaps exist.
- For new services, define the service (on the basis of business outcomes) and the service model.
- For changed services, define the impact on the service portfolio and existing service model and inform organisation.
- Publish service models that have been approved by the organisation.
- Perform periodic reviews of the service portfolio to ensure services remain aligned to business and IT strategies.
- Perform periodic reviews of the service portfolio to ensure that the ROI is still accurate.
- Conduct a review with the organisation of any services that are no longer aligned to the business and/or IT strategy or if the ROI has changed.

9.4.3 Service Provider

The service provider shall:
- Adhere to the defined and approved policy and process.
- Provide input (data, information and knowledge) to the service integrator for the definition and assessment of the new or changed service model.
- Provide service usage and cost data and information to the service integrator, on request, to aid the review of the service portfolio.

9.5 Financial Management Process

Financial management is defined by ITIL as: “A generic term used to describe the function and processes responsible for managing an organisation’s budgeting, accounting and charging requirements.”

This statement supports the Financial Management Process and covers all mandatory activities of the three main parties involved in the processes.

9.5.1 Organisation

The organisation shall:
- Define, make available and maintain the financial management process and policy.
- Communicate the financial management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the financial management policy results in a formal review, which may result in disciplinary action.

- Review financial impact of new / updated services.
- Develop new cost model or amend existing cost model, which both include definitions of:
  - How expenditure will be recorded and tracked
  - Item classification
  - Cost allocation
  - Recharge rules
  - Reporting and MI requirements
- Issue purchase order numbers to service providers for inclusion on their invoices.
- Perform assurance over the validation activities performed by the Service Provider and validate the Service Provider's invoice against the provided MI.
- Confirm with the service providers any manday effort chargeable prior to the service providers issuing appropriate invoices.
- Attend any invoice resolution reviews to discuss service provider invoice queries.
- Pay valid service provider invoices within the terms of the contract.
- Maintains and provide the recharge rules which specify which services are included in the central IT budget and which are recharged to the business units and how to calculate and apportion the costs appropriately to the consuming business units.
- Agree apportioned costs with business units and implement recharge by attributing the costs to the P&L of the individual business units.

9.5.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to service providers in fulfilling their financial management roles and responsibilities.
- Provide input at any stage of the cost model definition, due to their knowledge of the SIAM environment.
- Perform assurance over the validation activities performed by the Service Provider and validate the Service Provider's invoice against the provided MI.
- Review and validate invoices and management information provided by service providers for products and services, including service credits.
- Notify service providers of any discrepancies between invoices, supporting MI and the contract value for the service provided and reject any invalid invoices.
- Review invoice queries and provides recommendations on how to proceed. This could be a recommendation to pay in full, part-pay or not pay.
- Engage fully with service providers to resolve any invoice discrepancies.
- Attend any invoice resolution reviews to discuss service provider invoice queries.
- Provide a report of its findings in the review of service provider invoices to the organisation.
- Provide a consolidated statement of charges incurred by the organisation each service measurement period, supported by invoices and MI provided by service providers detailing the consumption of products and services by the organisation.
- Provide reports to the organisation providing recommendations on the apportionment of charges to the organisation's business units based on the apportionment model.
- Identify potential process improvements, make appropriate recommendations and coordinate improvement activities that span multiple service providers.
- Monitor and manage stakeholder compliance to the financial management policy, process and procedures and report any non-compliance.

9.5.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of procedures and supporting documentation.
- Raise invoices (including service credits) and associated supporting management information for products and service provided in accordance with the contract terms and conditions.
- Engage with the service integrator to resolve invoice discrepancies.
- Refund incorrect payments as soon as possible.
- Work with the service integrator and other service providers to assist with any engagement and non-compliance issues.

9.6 Service Design Coordination Process

Service design coordination is defined by ITIL as: "The process responsible for coordinating all service design activities, processes and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics."

This statement supports the Service Design Coordination Process and covers all mandatory activities of the three main parties involved in the processes.

9.6.1 Organisation

The organisation shall:

- Define, make available and maintain the service design coordination process and policy.
- Communicate the service design coordination policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the service design coordination policy results in a formal review, which may result in disciplinary action.
- Provide input to the definition of service timelines.
- Review service design plan and approve once finalised.
- Review service design package and approve once finalised
- Participate in providing mitigations to any risks to the design or design plan identified by the Service Integrator.

- Agree risk mitigations that have been proposed once reviewed and proven to be good.
- Participate in implementing agreed risk mitigations.

9.6.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Define contents of the service design package, timescales expected for the service, resources required to carry out the service design and calculate the cost of the design activities.
- Produce the design plan and issue once approved by the organisation.
- Initiate the design activities according to the design plan.
- Produce the service design package and issue to relevant resources once approved by the organisation.
- Monitor design activities and determine whether the design is on track, as per the design plan.
- Identify risks to the design or design plan, and inform organisation and service provider(s).
- Participate in providing mitigations to any risks to the design or design plan.
- Participate in implementing agreed risk mitigations.

9.6.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide input to the definition of timelines, resource requirements and cost estimates, if requested by the service integrator.
- Provide input to the service integrator on design plan delivery status, risks identified and potential risk mitigations.
- Participate in implementing agreed risk mitigations.

10 SERVICE PROVIDER ASSURANCE PROCESS STATEMENTS

10.1 Continual Service Improvement Process

Continual service improvement is defined by ITIL as: “A stage in the lifecycle of a service. Continual service improvement ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services and IT infrastructure in order to increase efficiency, effectiveness and cost effectiveness. Continual service improvement includes the seven-step improvement process. Although this process is associated with continual service improvement, most processes have activities that take place across multiple stages of the service lifecycle.”

This statement supports the Continual Service Improvement Process and covers all mandatory activities of the three main parties involved in the process.

10.1.1 Organisation

The organisation shall:

- Define, make available and maintain the continual service improvement process and policy.
- Communicate the continual service improvement policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the continual service improvement policy results in a formal review, which may result in disciplinary action.
- Inform the service integrator of potential service improvements.
- Provide input to prioritising improvement opportunities and decision on whether to continue as a CSI activity.
- Provide input to decide what should be measured in order to prove the success of the improvement initiative.
- Participate in defining / re-defining service improvement actions based on the high-level description of the initiative.
- Implement any service improvements allocated, based on the detailed description of the initiative and plan.
- Decide whether service improvements have been successful (based on information provided by service integrator) or if re-work is required.

10.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Collate and review all management information gathered from organisation and service providers and through continuous review of service management information flowing through the organisation.
- Provide input to prioritising improvement opportunities and decision on whether to continue as a CSI activity.
- Keep the CSI register up-to-date throughout the process.
- Discuss what should be measured, with organisation, in order to prove the success of the improvement initiative.
- Validate what can be measured in order to prove the success of the improvement initiative.
- Coordinate gathering of pre-implementation data and perform analysis to create a baseline upon which the success or failure of service improvement actions can be measured.
- Participate in defining / re-defining service improvement actions based on the high-level description of the initiative.
- Implement any service improvements allocated, based on the detailed description of the initiative and plan.
- Monitor all service improvement actions to completion.
- Coordinate gathering of post-implementation data and perform analysis to compare with baseline data and confirm whether the service improvement actions were a success or failure.
- Present results of service improvement initiatives to the organisation and relevant service providers.
- Communicate successful CSI initiatives to relevant stakeholders.

10.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Inform the service integrator of potential service improvements.
- Provide input to prioritising improvement opportunities and decision on whether to continue as a CSI activity.
- Participate in defining / re-defining service improvement actions based on the high-level description of the initiative.
- Implement any service improvements allocated, based on the detailed description of the initiative and plan.

10.2 Service Level Management Process

Service level management is defined by ITIL as: “The process responsible for negotiating achievable service level agreements and ensuring that these are met. It is responsible for ensuring that all IT service management processes, operational level agreements and underpinning contracts are appropriate for the agreed service level targets. Service level management monitors and reports on service levels, holds regular service reviews with customers and identifies required improvements.”

This statement supports the Service Level Management Process and covers all mandatory activities of the three main parties involved in the process.

10.2.1 Organisation

The organisation shall:

- Define, make available and maintain the service level management process and policy.
- Communicate the service level management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the service level management policy results in a formal review, which may result in disciplinary action.
- Provide input to validation of new / updated service levels and KPIs.
- Review the consolidated performance summary report and provide comments where necessary to the service integrator.
- Chair and manage the commercial and performance review meetings.

10.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide support and guidance to service providers in fulfilling their service level management roles and responsibilities.
- Monitor and manage stakeholder compliance to the service level management policy, process and procedures and report any non-compliance.
- Receive and validate requests for SLA adjustments and communicate outcome.
- Determine new or changed service level requirements and review with service provider.
- Convert service level requirements into service levels and KPIs and validate with organisation and service provider.
- Produce the service level agreement document, using the agreed service levels as input.
- Initiate contract negotiation and change and adjust service levels and service level agreement as contractually agreed.
- Communicate signed off SLAs and go-live dates to organisation and service provider.
- Review service provider management information each service measurement period and produce trend analysis and management summaries to identify service provider performance trends and potential performance opportunities and improvements.
- Provide expert input to periodic service level management audit reviews, as and when required.
- Produce and publish the weekly consolidated performance dashboard.
- Review and validate service provider claims for excused performance.
- Review service provider summary reports and produce and issue the consolidated summary report to the organisation.
- Collect information on service performance, calculate any performance credits and make recommendations to the organisation on performance credits.

10.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Assist the service integrator in the development of procedures and supporting documentation.
- Meet with service integrator to review and agree new or changed service level agreements.
- Provide the service integrator with a service level report / management information, in each service measurement period, in accordance with the service level management policy, process and procedures.
- Provide input to validation of new / updated service levels and KPIs.
- Monitor and analyse service level / KPI performance and provide evidence and trend analysis to the service integrator within an agreed number of days of the end of each service management period.
- Work with the service integrator and other service providers to assist with any service provider engagement and non-compliance issues.
- Provide input to periodic service level management audit reviews when required.
- Provide weekly dashboard information to the service integrator.
- Undertake checks to ensure performance data provided to the service integrator is accurate and complete.
- Address and resolve any queries with the service measurement period reports raised by the service integrator.

11 SERVICE TRANSITION SUPPORT PROCESS STATEMENTS

11.1 Release Management Process

Release Management is defined by ITIL as: "The process responsible for planning, scheduling and controlling the build, test and deployment of releases and for delivering new functionality required by the business while protecting the integrity of existing services."

This statement supports the Release Management Process and covers all mandatory activities of the three main parties involved in the process.

11.1.1 Organisation

The organisation shall:

- Define, make available and maintain the release management process and policy.
- Communicate the release management policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the release management policy results in a formal review, which may result in disciplinary action.
- Provide input to definition of preliminary release scope and schedule.
- Review and approve the release plan.
- Take part in operational / deployment readiness reviews to ensure that the organisation and relevant service providers have the required skills to consume the release and its functionalities.
- Attend the post-release review and review the published post-release report.

11.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Develop, maintain and communicate the release management strategy.
- Receive release candidate information and define the preliminary release scope and schedule with input from the organisation.
- Produce the release plan and publish once approved by the organisation.
- Organise and conduct operational / deployment readiness reviews to ensure that the organisation and relevant service providers have the required skills to consume the release and its functionalities.
- Manage the implementation and confirm service providers and organisation readiness to proceed with project go-live.
- Ensure releases are packaged in accordance with the release management strategy.
- Manages and coordinate ELS to ensure that end-to-end support is efficiently accomplished, and goverance is adhered to. Agree the scheduling of fixes with the service provider and organisation.
- Produce and publish an ELS closure report.
- Organise and conduct the post-release review and produce and publish the post-release report.
- Verify deployment has been successfully completed to all relevant stakeholders and close the release.

11.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Build the release packages as defined in the published release plan and in-line with whatever is specified in the release policy.
- Perform allocated activities as per the draft consolidated implementation plans.
- Provide product catalogue, release plans and roadmaps to the service integrator.
- Package releases in accordance with the release management strategy.
- Take part in operational / deployment readiness reviews to ensure that the organisation and relevant service providers have the required skills to consume the release and its functionalities.
- Provide early life support immediately after deployment.
- Attend and contribute to the post-release review and review the published post-release report.

11.2 Transition Planning and Support Process

Transition planning and support is defined by ITIL as: "The process responsible for planning all service transition processes and coordinating the resources that they require."

This statement supports the Transition Planning and Support Process and covers all mandatory activities of the three main parties involved in the process.

11.2.1 Organisation

The organisation shall:

- Define, make available and maintain the transition planning and support process and policy.
- Communicate the transition planning and support policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the transition planning and support policy results in a formal review, which may result in disciplinary action.
- Review and approve the plan to deliver service transition.
- Maintain the overall project plan that incorporates the service delivery transition plan.
- Participate in post-project reviews.
- Provide the required project documentation to facilitate environment provision.
- Approve the costed approval and provide environment sign-off criteria.
- Confirm authority to proceed with project go-live.

11.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.

- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Engage with service providers and organisation project staff throughout the process.
- Produce and maintain a plan to deliver service transition and agree the plan with service providers.
- Provide status updates on progress towards the delivery of the service transition plan.
- Consolidate the service providers' delivery plans into the service transition delivery plan and manage the delivery plans.
- Engage with service providers to review transition requirements and produce the transition approach.
- Consolidate service providers transition plans into a project transition plan and provide regular update reports of progress against the plan to the organisation.
- Manage the consolidated project transition plan and confirm all activities and products are in place for the operational readiness review.
- Manage the operational handover from the project team to the organisation and operational service providers.

11.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Review and approve the plan to deliver service transition.
- Complete all assigned activities in the service transition delivery plan.

12 SERVICE VALIDATION AND TEST PROCESS STATEMENTS

12.1 Service Validation and Test Process

Service validation and testing is defined by ITIL as: “The process responsible for validation and testing of a new or changed IT service. Service validation and testing ensures that the IT service matches its design specification and will meet the needs of the business.”

This statement supports the Service Validation and Test Process and covers all mandatory activities of the three main parties involved in the process.

12.1.1 Organisation

The organisation shall:

- Define, make available and maintain the service validation and test process and policy.
- Communicate the service validation and test policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the service validation and test policy results in a formal review, which may result in disciplinary action.
- Provide input to the assessment of the service design package (SDP) or request for change (RFC).
- Provide approval of service test strategy / approach, test resources and schedule.
- Define test plan / scenarios and tool set up with service provider.
- With the service provider, review acceptance test plan, perform acceptance testing and provide acceptance test reports.
- Perform service management acceptance testing with the service provider.
- Provide agreement on operational acceptance test (OAT) and service management acceptance test (SMAT) reports.
- Sign-off all testing with the service integrator.
- Identify potential process improvements and feed back to service integrator.

12.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Lead the assessment of the SDP or RFC.
- Define and publish the service test strategy and approach.
- Collate resources, costs and schedule.
- Assure that test plan and scenarios are completed.
- Initiate and authorise unit testing, system testing, integration testing and acceptance testing, if required.
- Collate OAT and SMAT reports for a cross-provider release.
- Ensure all testing exit critera are met or waivers provided.
- Collate all test reports.
- Sign-off all testing with the organisation.
- Collate all potential process improvements and feed into Continual Service Improvement Process.

12.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide input to definition of the service test strategy and approach.
- Define resources, costs and schedule and forward to service integrator.
- Define test plan / scenarios and tool set up with organisation.
- Perform unit testing, system testing and integration testing, rectify identified defects and provide test reports to service integrator.
- With the organisation, review acceptance test plan, perform acceptance testing, provide acceptance test reports and rectify any defects.
- Perform operational acceptance testing, rectify defects and provide test reports to service integrator.
- Perform service management acceptance testing with the organisation, rectify defects and provide test reports to service integrator.
- Upload test documentation in the SKMS.
- Identify potential process improvements and feed back to service integrator.

13 IT INFORMATION SECURITY PROCESS STATEMENTS

13.1 Information Security Management Support Process

Information security management is defined by ITIL as: "The process responsible for ensuring that the confidentiality, integrity and availability of an organisation's assets, information, data and IT services match the agreed needs of the business. Information security management supports business security and has a wider scope than that of the IT service provider and includes handling of paper, building access, phone calls, etc. for the entire organisation."

This statement supports the Information Security Management Support Process and covers all mandatory activities of the three main parties involved in the processes.

13.1.1 Organisation

The organisation shall:

- Define, make available and maintain the information security management processes, policies and standards.
- Perform a security risk assessment and define security controls.
- Communicate the information security management policies, processes and standards to the service integrator and all relevant stakeholders.
- Ensure that non-adherence to the information security management support policy results in a formal review, which may result in disciplinary action.
- Coordinate security training and awareness sessions.
- Provide assurance that the design and build of the service are aligned to the security standards and policies and provide approval, advice and/or guidance on any identified exceptions.
- Approve monthly information security reports.
- Review and approve / reject security incident counter-measures or corrective actions.
- Implement security counter-measures or corrective actions, where required.
- Review and approve security incident reports.

13.1.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Provide input to the creation of information security policies, information security management framework and definition of security controls.
- Publish the information security management policies, information security management framework and security controls.
- Align their security policies to the organisation's information security standards and policies.
- Create new / modify existing standards and procedures for security mechanisms to be supported across delivery teams and provide to organisation.
- Review service providers' new / modified standards and procedures and forward to organisation.
- Reviews the design and build of the service, confirm that it is aligned to the organisation's security standards and policies and provide advice / guidance on any exceptions identified.
- Escalate to the organisation to accept the design and any exceptions identified.
- Monitor the security systems and security landscape.
- Coordinate the following reviews:
  - Analysis of previous security breaches and incidents.
  - Periodic review of security policies.
  - Periodic review of security mechanisms and procedures.
  - Major incident reports.
  - Threats and security controls.
  - Findings from security testing.
- Prepare the consolidated IS review reports against the defined SLAs and KPIs and forward to the organisation for review and approval.
- Documents detected security failures, threats and/or weaknesses.
- Identify areas of opportunity where security measures must be enhanced.
- Lead the review, impact assessment and preparation of counter-measures / corrective actions for security incidents.
- Implement security counter-measures or corrective actions, where required.
- Prepare and publish security incident reports.

13.1.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide input to the creation of information security policy and controls.
- Align their security policies to the organisation's information security standards and policies.
- Create new / modify existing standards and procedures for security mechanisms to be supported across delivery teams and provide to service integrator.
- Review security and provide reports, as requested by the service integrator, which contain a summary of all security reviews.
- Support and provide input to the review, impact assessment and preparation of counter-measures / corrective actions for security incidents.
- Implement security counter-measures or corrective actions, where required.

13.2 Accreditation Support Process

Accreditation is the formal assessment of an information system against its information assurance requirements, resulting in the acceptance of residual risks in the context of the business requirement. Accreditation must be an informed decision, made in full understanding of the

implications and taken at the right level of management. Appropriate service accreditation is a prerequisite for receiving approval to operate. Accreditation must be reviewed periodically throughout the service life of the information system.

This statement supports the Accreditation Support Process and covers all mandatory activities of the three main parties involved in the processes.

13.2.1 Organisation

The organisation shall:

- Adhere to the group security policies, standards and procedures.
- Review the security policies, standards and procedures and provide comments to the service integrator.
- Approve any changes to the security policies, standards and procedures.
- Provide all necessary project information and assistance required by the service integrator to support the security accreditation process.
- Review and comment on risk assessments and reports provided by the service integrator.
- Ensure risk owners are identified for all security risks raised by the service integrator.
- Provide all necessary business information and assistance required by the service integrator to support the security audit process and schedule.
- Review and comment on the annual statement of control and vulnerability provided by the service integrator.
- Attend security awareness sessions and workshops and other specialist security meetings organised by the service integrator.
- Define, make available and maintain the accreditation support process and policy.
- Communicate the accreditation support policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the accreditation support policy results in a formal review, which may result in disciplinary action.

13.2.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Adhere to the group security policies, standards and procedures.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Keep abreast of changes in HMG security policies and security standards that have relevance for the organisation.
- Maintain comprehensive knowledge of influences on the organisation's security stance.
- Review security policies, standards and procedures, at least annually, in light of evolving standards, the organisation's IT and related strategies, service provider views and industry best practice.
- Identify, recommend and impact and communicate changes required to security policies, standards and procedures and update accordingly when agreed with the organisation.
- Perform risk assessments, business impact assessments and produce risk reports for all projects undergoing accreditation using HMG information assurance standard risk assessment methodology or other methodology, agreed with the organisation.
- Maintain accreditation status.
- Proactively monitor and progress completion of all required accreditation documentation and resolution of security issues, including reporting and escalation to the organisation as required.
- Monitor, investigate and assess the cumulative effect on the organisation's business of all IT security risks reported from agreed sources.
- Advise the organisation and service providers on how those risks can be mitigated and track action plans to mitigate those risks.
- Provide risk assessments on all requests by service providers to off-shore activities that could breach the organisation's policies and make recommendations to the organisation regarding the acceptability of the risks identified.
- Act as the organisation's agent in providing, withholding or qualifying consent on behalf of the organisation where a service provider requires authorisation before embarking on a course of action in connection with the provision of security services.
- Act as a central point for the receipt of requests from the organisation for covert access, e.g. In connection with reports of abuse.
- Facilitate or enable the provision of such covert access as may be reasonably requested by the organisation from time-to-time to assist in the investigation of a user.
- Monitor service provider compliance with the organisation's security policies, standards and processes and advise service providers of the action required to resolve the non-compliance and monitor progress toward completion of the recommendations within a timeframe agreed with the organisation.
- Develop, maintain and undertake a programme of security audits to provide appropriate assurance of service provider compliance with the organisation's security policies, standards and processes.
- Produce an annual statement of control and vulnerability incorporating information gathered throughout the year from the sources monitored to inform future security improvement activities.
- Propose scope and format / delivery mechanism of a security awareness programme for the organisation and service provider staff.
- Develop and maintain appropriate supporting material (e.g. presentations, intranet inserts, posters and leaflets), consistent with any organisation internal awareness programme and strategy and undertake security awareness as agreed with the service provider.
- Develop a communications plan to effectively exploit the organisation's internal communications tools as a means of publicising changes to security policies, standards and procedures and of notifying other

information that may reasonably be required by the organisation to be posted.

13.2.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Adhere to the group security policies, standards and procedures.
- Review the security policies, standards and procedures and provide comments to the service integrator.
- Provide all necessary information and assistance required by the service integrator to support the security accreditation process.
- Put in place and actively manage remedial actions to resolve any issues discovered by the service integrator in its accreditation assessment.
- Actively monitor and minimise security risks known to the service provider or highlighted by the service integrator.
- Assist the service integrator in security audits by providing all necessary information, data and resource to enable the service integrator to perform its audits.
- Put in place and actively manage remedial actions to resolve any issues discovered by the service integrator as part of its audit activity.
- Attend security awareness sessions and workshops and other specialist security meetings organised by the service integrator.

13.3 Crypto Service Process

The management, allocation and distribution of security keys is, to a high degree, the responsibility of individual suppliers and will form part of their service provision. However, there remains a critical requirement for the overall governance and management of keys as this will ensure that service provision, access to software and resources and availability is not compromised by mismanagement.

This statement supports the Crypto Service Process and covers all mandatory activities of the three main parties involved in the processes.

13.3.1 Organisation

The organisation shall:

- Define, make available and maintain the crypto service process and policy.
- Communicate the crypto service policy and process to the service integrator and the service providers.
- Ensure that non-adherence to the crypto service policy results in a formal review, which may result in disciplinary action.
- Provide new key requirements / requests for change of existing security keys to the service integrator.
- Review design requirements received from the service integrator and decide whether or not to approve.
- Review any improvement actions suggested by the service integrator and decide whether or not to approve.

13.3.2 Service Integrator

The service integrator shall:

- Adhere to the defined and approved policy and process.
- Produce the relevant procedures and supporting documentation to support the delivery of the process.
- Identify, document and design functional requirements.
- Monitor industry mandates and emerging key management standards and propose application of these to the crypto service.
- Defines consistent procedures to manage keys across all suppliers and initiate and manage the solution and design activities required.
- Create keys as per service requests.
- Ensure appropriate policy, process, technology documents and keys are stored in a centralised secure location for all towers.
- Ensure that the Release Management Process is followed for any releases relating to the crypto service.
- Ensure that keys are delivered to the authorised operator, responsible for ownership and management of keys, in cooperation with the service integrator.
- Monitor performance (e.g. data corruption and unavailability), deployed keys in the production environment and unauthorised access to crypto systems.
- Distribute crypto service reports to relevant stakeholders
- Conduct periodic internal audits and coordinate with the CSI team for internal audit.
- Coordinate external audits to verify that the service is compliant with the specified security standards and policies, as required.
- Appoint an external accredited body for external audits, if required by the organisation.
- Maintain a central repository to store audit reports.
- Analyse audit reports, document any potential improvement actions and send to the organisation for review.
- Engage with the CSI team to action any agreed recommendations resulting from audits.

13.3.3 Service Provider

The service provider shall:

- Adhere to the defined and approved policy and process.
- Provide new key requirements / requests for change of existing security keys to the service integrator.
- Design the key, as per the functional design requirements and protect it using appropriate encryption methods.
- Creates and make available the underpinning security policies.
- Ensure all security requirements are addressed as per the functional design requirements and confirm that the requirements can be fulfilled,
- Specify any pre-conditions which must be fulfilled, checked and verified before the service can be made operational.

- Ensure appropriate technology solutions and related documents are created and made available.
- Provide any required input to the service integrator to create the keys.
- Receive the key from the service integrator and coordinate the deployment of new keys and associated archiving of decommissioned keys.
- Provide reports to the service integrator on performance of the crypto service, in accordance with the agreed reporting requirements.
- Establish and maintain a measurement process across its services, in accordance with the service integrator's procedures.

14 GLOSSARY

BCP	Business Continuity Planning
CAB	Change Advisory Board
CFIA	Component Failure Impact Analysis
CI	Configuration Item
CIO	Chief Information Officer
CMDB	Configuration Management Database
CSI	Continual Service Improvement
DR	Disaster Recovery
ELS	Early Life Support
HMG	Her Majesty's Government
IS	Information Security
IT	Information Technology
ITIL	IT Infrastructure Library
ITSC	IT Service Continuity
ITSCM	IT Service Continuity Management
ITSM	IT Service Managememnt
KPI	Key Performance Indicator
MI	Management Information
OAT	Operational Acceptance Test(ing)
P&L	Profit and Loss
PIR	Post Implementation Review
QBF	Quarterly Business Forecast
QCP	Quarterly Capacity Plan
RFC	Request for Change
ROI	Return on Investment
SDP	Service Design Package
SIAM	Service Integration and Management
SKMS	Service Knowledge Management System
SLA	Service Level Agreement
SMAT	Service Management Acceptance Test(ing)
SOC	Security Operations Centre
SPOF	Single Point Of Failure
TSOM	Target Service Operating Model
VSAC	Volume of Services Actually Consumed