This is a DRAFT document, being published for review & comment

The content is therefore subject to change & revision

This document is part of the XGOV Strategic SIAM reference set

It includes the Future SIAM model with detailed service descriptions

The document is part of a consistent approach to SIAM

enabling central government & other public sector organisations

to apply SIAM flexibly to meet the specific needs in each implementation

Please send your feedback to SIAM@gps.gsi.gov.uk

Service Integration & Management (SIAM) Framework

Cross Government Reference Set

SIAM Enterprise Model

Enterprise Architecture

Includes:
- Architecture Vision & Design
- Architecture Policy & Standards
- Architecture Roadmap & Plans
- Architecture Management

Policy & Standards Mgt (inc Security)

Programme Mgt & Governance

Includes:
- Overall Direction & Support
- Programme Risk Management
- Project Management Standards

Systems Integration

Includes:
- Requirements Development
- Validation
- Integrated Project Management
- Project Risk Management
- Decision Analysis & Support

2. Service Desk

2.1 Service Desk General, 2.2 Incident, 2.3 Request Management
2.4 Problem Management, 2.5 Access Management

1. Core SIAM - Service Integration & Management

1.1 Availability Management
1.2 Capacity Management
1.3 Change Management
1.4 Event Management
1.5 IT Service Continuity Mgt
1.6 Service Asset & Configuration
1.7 Service Catalogue Management
1.8 Service Level Management
1.9 Standards and Architecture
1.10 Financial Management Support
1.11 Service Provider Management

3. Service Knowledge Mgt

Central Repository for all Service Management Reference material

4. Service Provider Assurance

4.1 Service Level Design & Review
4.2 Service and Supplier quality
4.3 Regulatory Service Provider Compliance

5. IT Info Security Support

5.1 Incident & Event Monitoring
5.2 Protective Monitoring
5.3 Forensic Analysis
5.4 Security Assurance / Accreditation

6. Service Transition Planning & Design

6.1 Service Transition Planning
6.2 Project Management
6.3 Release & Deployment Mgt
6.4 Transformation Delivery & Cost Optimisation

7. Service Validation & Testing

7.1 Test Planning & Design
7.2 Service Evaluation
7.3 Test Environment Management

Retained Controls:

- Procurement and Contract Mgt
- Vendor Management
- Exit Management
- Service / Solution Assurance
  - Requirements Development
  - Decision Analysis & Support
  - Assurance & Validation
- Service Strategy & Architecture
- Demand Management
  - Business Service Catalogue
  - Business Relationship Mgt
  - Business Architecture
- Financial Management
- Service Portfolio Management
- Risk Management

Service Towers: **eg** Desktop Services, Hosting Services, Network Services (PSN), Cloud Services

Retained Organisation | Retained supported by managed service | SIAM services | Services

SIAM Services

2. Service Desk

2.1 Service Desk General, 2.2 Incident, 2.3 Request Management 2.4 Problem Management 2.5 Access Management

1. Core SIAM - Service Integration & Management

1.1 Availability Management
1.2 Capacity Management
1.3 Change Management
1.4 Event Management
1.5 IT Service Continuity Mgt
1.6 Service Asset & Configuration
1.7 Service Catalogue Management
1.8 Service Level Management
1.9 Standards and Architecture
1.10 Financial Management Support
1.11 Service Provider Management

3. Service Knowledge Mgt

Central Repository for all
Service Management
Reference material

4. Service Provider Assurance

4.1 Service Level Design & Review
4.2 Service and Supplier quality
4.3 Regulatory Service Provider Compliance

5. IT Info Security Support

5.1 Incident & Event Monitoring
5.2 Protective Monitoring
5.3 Forensic Analysis
5.4 Security Assurance / Accreditation

6. Service Transition Planning & Design

6.1 Service Transition Planning
6.2 Project Management
6.3 Release & Deployment Mgt
6.4 Transformation Delivery & Cost Optimisation

7. Service Validation & Testing

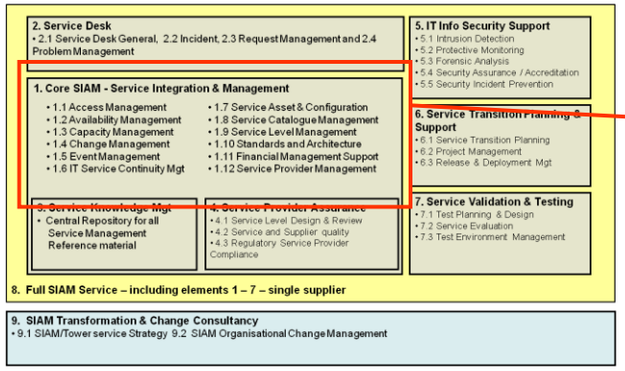
7.1 Test Planning & Design
7.2 Service Evaluation
7.3 Test Environment Management

8. Full E2E SIAM Service (1 to 7) single supplier: over 5,000 users

9. Full E2E SIAM Service (1 to 7) single supplier: upto 5,000 users

10. SIAM Transformation Design & Change Consultancy

1. Core SIAM Service



1. Core SIAM - Service Integration & Management

- 1.1 Availability Management
- 1.2 Capacity Management
- 1.3 Change Management
- 1.4 Event Management
- 1.5 IT Service Continuity Mgt
- 1.6 Service Asset & Configuration
- 1.7 Service Catalogue Management
- 1.8 Service Level Management
- 1.9 Standards and Architecture
- 1.10 Financial Management Support
- 1.11 Service Provider Management

Description

This provides the core SIAM service for IT operational management of the delivery of the services.
Core SIAM Services co-ordinates and consolidates the management of individual services from Service Providers providing end-to-end service management whilst ensuring that services consistently meet business objectives and requirements for performance, quality and cost. Core SIAM Services includes the above functions and processes.

Core SIAM Services also includes the provision of Integrated ITSM tooling providing interface and data policies and standards that facilitate all Service Provider feeds into a central data hub with full communications exchange to enable SIAM to manage the end-to-end service in real time.

1.1 Availability Management

Description

Availability Management has to ensure that the delivered availability levels for all services comply with or exceed the agreed requirements in a cost-effective manner

Outcomes

- Provide and improve the end-to-end availability of the Department's critical business systems and services
- Measure and report on the average and maximum end-to-end response times for the Department's critical systems transactions
- To record, analyse and reduce the frequency at which the IT services and systems fail

Relationship & Interfaces

Customer/Service Consumer

- Provide impact assessments where required to SIAM

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Availability Management Policies and Procedures.
- 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 Policies and Procedures.
- Co-ordinate any proposed improvement activities that span multiple Service Providers
- Monitor and manage stakeholder compliance to the Availability Management Policies and Procedures and inform Service Providers of any material non-compliance with the Availability Management Policies and Procedures
- Receive notification of new/amended availability requirements and initiate impact assessment
- Identify and inform the Service Providers of the end-to-end measurement elements that need to be measured by the Service Providers in the reporting against the end-to-end service availability target
- Monitor, analyse and calculate the performance of Service Providers against the end-to-end KPIs, consolidate and report to the Department
- Provide a consolidated report to the Department for the measurement of the defined Departmental critical business transactions
- Attend Service Delivery Review meetings to discuss the availability management content of the dashboard and provide reports
- Review the end-to-end KPIs with the Department and document and communicate any areas for improvement to the Service Providers

Service Provider

- Assist SIAM in the development of the Availability Management Policies and Procedures
- Assist SIAM in the creation of the end to end pictorial component and application overview to enable the development and ongoing maintenance of the Availability Plan
- Review and approve the Availability Plan provided by SIAM
- Evaluate the effectiveness of its own availability management process and implement changes to its availability management process to improve efficiency
- Work with SIAM and other Service Providers to assist with any Service Provider engagement and non-compliance issues
- Provide SIAM with a detailed impact for new/amended availability requirements
- Provide application/service availability data to SIAM to enable the measurement of end-to-end availability
- Provide the required data feeds to SIAM for the measurement of the defined Departmental critical business transactions
- Undertake Component Failure Impact Analysis (CFIA) and Single Points of Failure (SPOF) analysis

Key metrics

- Not Applicable

Key metrics

- Achieve a minimum End-to-end availability of x% for all Department critical IT service and systems each Measurement Period
- Reduce the frequency at which IT services and systems fail by x% year on year
- Reduce the impact to Department users customers of failure of IT services and systems measured in Business Days year on year by x%

Key metrics

- Achieve contractual Service Levels and Service Targets for systems availability for all Department critical systems each Measurement Period

1.2 Capacity Management

Description

Capacity Management has to provide IT capacity coinciding with both the current and future needs of the customers balanced against justifiable costs

Outcomes

- Ensure the optimum amount of IT capacity is provided to meet the Department's needs
- Accurately forecast resource demands based on the Department's business forecasts and provide accurate, qualitative management reporting of current and future Service capacity status
- Analyse Supplier management information 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
- Provide real-time on demand capacity provisioning
- Reduce the number of queries raised by the Department against Supplier Capacity Plans and forecasts
- Improve service to customers by minimising business disruption caused by Capacity limitations

Relationship & Interfaces

Customer/Service Consumer

- Provide insight into the Department's current and future business events and strategy which may impact capacity
- Provide to SIAM the Department's Quarterly Business Forecast (QBF) and any other related Departmental IS/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)
- Classify each opportunity optimisation suggestion as either "accepted", "rejected" or "requiring further information" and if "rejected" provide reasons for the rejection
- Where appropriate ensure that the correct commercial contract is in place and ensure that funding is available to progress the optimisation opportunity

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Capacity Management Policies and Procedures.
- Provide support and guidance to the Department and its Service Providers in fulfilling their capacity management roles and responsibilities
- Progress all capacity related issues raised by the Department with the appropriate Service Providers
- Manage through any cross-Service Provider issues that cannot be resolved directly between the Service Providers
- Proactively identify capacity management process improvements, make appropriate recommendations to Service Providers and co-ordinate improvement activities that span multiple Service Providers
- Monitor and manage stakeholder compliance to the Capacity Management Policies and Procedures and inform Service Providers of any Service Provider material non-compliance
- Co-ordinate capacity planning activities that span multiple Service Providers ensuring that forecast and actual data is realistic and appropriate and facilitates the identification of remedial action by, and between Service Providers
- Distribute Quarterly Business Forecasts (QBF) to the Service Providers ensuring that key changes that need to be reflected in the Service Provider's Quarterly Capacity Plans (QCP) and Resource Unit forecasts are identified accurately
- Provide assurance to the Department that QCP narratives and Resource Unit forecasts are realistic and align with Departmental forecasts, IS/IT Strategies and reflect known Project engagement
- Review Service Provider QCP plans to ensure that opportunities for capacity optimisation have been included and where appropriate challenge the Service Provider where no, or 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

Service Provider

- Assist SIAM in the development of the Capacity Management Policies and Procedures
- Ensure that appropriate levels of monitoring of resources and system performance are set and that information recorded is kept up to date
- Provide insight into performance achieved 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 SIAM any cross-Service Provider issues that cannot be resolved directly between the Service Providers
- Work with SIAM 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 SIAM on capacity volumes and trends
- Analyse the Quarterly Business Forecasts (QBF) and provide their Quarterly Capacity Plan (QCP) in the required format to SIAM
- Ensure that forecast narratives and data are realistic, consistent and align with Departmental business forecasts, IS/IT Strategies and reflect known Project engagement

1.2 Capacity Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Ensure that the wider Departmental 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 suggestedby Service Providers that includes the status of each suggestion • Discuss Service Providers proposals for optimisation with Service Providers and the Department and create an Optimisation Opportunity Analysis Report describing the opportunity, proposed benefits, findings and outcome • Where optimisation opportunities are approved by the Department, monitor Service Providers progress against 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	• Ensure the QCP demonstrates an understanding between business demand, use of IT related services and Resource Unit consumption • Identify opportunities for optimising capacity in QCP plans 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 SIAM/the Department as appropriate • When approved, produce a plan for implementation of the proposed optimisation opportunity and manage the activities within the plan through to a successful conclusion, reporting progress and any issues to SIAM as they occur • Where required provide information to SIAM 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 impacting process for analysing server capacity requirements as a result of a business change provided by the Department • Ensure that the forecast narrative provides sufficient information to enable the Department to understand the risks and consequences associated with any action/inaction, the timescales until problems will be experienced and recommended mitigation action to eliminate or minimize impacts, the likely costs associated with remedial options/action and the decisions required by the Department
Key metrics	**Key metrics**	**Key metrics**
• Percentage of Departmental Quarterly Business Forecasts provided on time • Percentage of capacity optimisation opportunities approved	• Year on year percentage reduction of x% in the number of queries raised by the Department against the consolidated quarterly capacity plan • Year on year percentage reduction of x% in the number of queries raised by the Department against the volume of services actually consumed report • At least x% of resource unit forecasts measured in the volume of services actually consumed report are within the expected levels of accuracy per Measurement Period	• Percentage of Quarterly Capacity Plans produced on time • Percentage of Quarterly Capacity Plans produced to sufficient quality • Percentage of queries raised by SIAM against the Quarterly Capacity Plan • Percentage of queries raised by SIAM against the Volume of Services Actually Consumed report • Percentage of capacity optimisation opportunities provided to SIAM

1.3 Change Management

Description

The primary objective of Change Management is to enable beneficial changes to be made, with minimal disruption to IT services. Change Management ensures that changes are deployed in a controlled way, i.e. they are evaluated, prioritised, planned, tested, implemented and documented

Outcomes

- Improve service to customers by minimising incidents and business disruption caused by Change activity
- Improve the rate of change success year on year by ensuring rigorous management of the Change process
- Maintain a 2 year forward schedule of change for the Department taking account of all planned changes and releases covering both business change and infrastructure change
- Improve the visibility and communication of change activity to the Department and service support staff including the tracking and visibility of all Changes regardless of whether they are managed through the formal Change Management process

Relationship & Interfaces

Customer/Service Consumer

- Provide Impact Assessments of RFCs where required

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Change Management Policies and Procedures.
- 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 Change Assurance Board meetings including emergency meetings
- Review assessment groups for change impacting for appropriateness and advise of other areas that will need to impact the change
- Ensure that any issues raised at the Change Assurance Board meeting are progressed satisfactorily
- Ensure change records are updated throughout their lifecycle and in line with the decisions made at the Change Assurance Board
- Following implementation of a change, ensure that Post Implementation Reviews are managed effectively
- Develop, manage, maintain and communicate to stakeholders the Department's Forward Schedule of Change and the Projected Service Availability document
- Review Service Provider management information and produce its own expert trend analysis and management summaries to identify change volumes and trends for discussion with the Department and the Service Providers at the appropriate forums

Service Provider

- Assist the Service Integrator in the development of the Change Management Policies and Procedures Log and track changes during their lifecycle
- Ensure that Requests for Change (RFCs) submitted are completed
- Ensure that any RFC raised has sufficient justification and are submitted in sufficient time to avoid the need for SIAM to initiate urgent action to ensure the change is implemented to the required timescale
- Ensure the RFC record is updated during its lifecycle and contains the accurate CAB score prior to be issued for impact assessment
- 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 RFCs are scheduled to protect overtime for the Department where possible
- Ensure that any cancelled RFC identified the reasons for the cancellation

1.3 Change Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	▪ Identify potential process improvements, make appropriate recommendations to Service Providers and manage through any process improvement activity ▪ Monitor and manage Service Providers compliance to the Change Management Policies and Procedures and inform Service Providers of any Service Provider material non-compliances	▪ Provide input to CAB by:- o Providing suitably empowered representation; o Ensuring all management summaries are submitted by the required date and time and meet the required entry criteria o Ensure that notification of the approval decision is disseminated as appropriate within its own organisation o 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 Post Implementation Review (PIR) is completed and any actions arising from the PIR are progressed accordingly ▪ Ensure that the outcome of any implementation activity is detailed on the RFC ▪ Ensure that the change is closed with an accurate closure code ▪ Monitor, analyse and report to SIAM on change volumes and trends ▪ Implement any resulting improvement activity ▪ Work with SIAM and other Service Providers to assist with any Service Provider engagement and non-compliance issues
Key metrics	**Key metrics**	**Key metrics**
• Not Applicable	• Year on year percentage improvement in changes successfully deployed each Measurement Period- • Less than x% of incidents each Measurement Period caused by changes deployed • Less than x% of lost or disrupted service availability as a result of changes deployed • Less than x% of incidents each Measurement Period caused by failed changes • x% of changes implemented must have been correctly impacted, scored and categorised	• Percentage of changes successfully deployed each Measurement Period • Percentage of incidents each Measurement Period caused by changes deployed • Percentage of lost or disrupted service availability as a result of changes deployed • Percentage of incidents each Measurement Period caused by failed changes

1.4 Event Management

Description

Event Management is the process that monitors all events that occur through the IT infrastructure to allow for normal operation and also to detect and escalate exceptional conditions. Event Management can be automated to trace and escalate unforeseen event circumstances

Outcomes

- Ensure Suppliers have appropriate monitoring in place to detect events in the IT infrastructure
- Improve the service provided to customers by minimising the impact of business disruption caused by events
- Comply with the Department's Systems Management Strategy

Relationship & Interfaces

Customer/Service Consumer

- Notify SIAM when it becomes aware of an Event
- Assist Service Providers and SIAM in the investigation of such Events

SIAM (Outsourced or Retained)

- Log, consolidate and analyse activity on agreed devices on the Department'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
- In all cases ensure where a service risk is identified the Service Providers take remedial action as necessary and agreed with the Department - including where appropriate co-ordinating the activities of the Service Providers involved
- Receive and record all events and incidents

Service Provider

- Notify SIAM when it becomes aware of an Event and provide all necessary details and information of such Event
- Investigate, contain, track, manage and resolve Events

Key metrics

Key metrics

Key metrics

1.5 IT Service Continuity

Description

IT Service Continuity Management (ITSCM) has to support business continuity by ensuring that the required IT facilities (computer systems, networks etc) can be resumed within the agreed timeframe

Outcomes

- Ensure that IT Service Continuity tests are successfully performed in accordance with the Department's IT Service Continuity Programme
- Ensure that Suppliers have robust and current IT Service Continuity Plans in place
- Ensure Suppliers undertake IT Service Continuity threat assessments

Relationship & Interfaces

Customer/Service Consumer

- Review and agree the ITSCM Policy
- Review and agree the ITSCM Strategy
- Agree the ITSCM Test Programme with SIAM
- Agree the ITSCM test scope
- Attend stakeholder meetings as appropriate and ensure any customer actions are completed
- Provide business input to the ITSCM risk process
- Provide business input to the ITSCM test
- Provide a decision on whether or not an ITSCM event should be declared

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the IT Service Continuity Management (ITSCM) Policies and Procedures.
- Provide support and guidance to DWP and its Service Providers in fulfilling their IT Service Continuity Management roles and responsibilities
- Produce the ITSCM Policy, agree this with the Department and reset the Policy at least annually
- Produce the ITSCM Strategy, agree this with the Department and reset the Strategy at least annually
- Manage the ITSCM Risk process
- Progress all ITSCM related issues raised by the Department with the appropriate Service Provider
- Ensure ITSCM awareness activity is conducted both within the SIAM team and across the Service Provider community
- Monitor and manage stakeholder compliance to the IT Service Continuity Management Policies and Procedures and inform Service Providers of any Service Provider material non-compliances
- Review Service Provider IT Service Continuity management information on and produce its own expert trend analysis and management summaries to identify ITSCM issues and trends for discussion with the Department 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 Department and reset the ITSCM Plan at least annually and maintain to ensure its currency
- Develop and agree the ITSCM Test Programme with the Department 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

Service Provider

- Assist SIAM in the development of the IT Service Continuity Management Policies and Procedures
- Conduct ITSC awareness activity within the Service Provider ITSC team
- Work with SIAM 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 inform SIAM of the outcome
- Analyse Root Cause Analysis and Incident Closure Reports and inform SIAM of the outcome and raise any current and emerging ITSCM risks required
- Produce the Service Provider ITSC Plan and agree it with SIAM
- 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 those risks
- Produce and update ITSC products including Test Recovery Plans as appropriate
- Provide information to SIAM to assist in the completion of the ITSC Test Programme
- Contribute to the high level ITSC Test Plan and produce its own low level test plans
- Analyse the test 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

1.5 IT Service Continuity

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider

	• Produce and agree with Service Providers and the Department the ITSCM test scope and overarching 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 as required
	  ○ prepare event options and recommendations for consideration by the Department;
	  ○ direct recovery plan activity;
	  ○ prepare a plan to return to normal operations within x days of an ITSCM event being declared
		• During both the execution of a ITSCM Test Plan and the execution of a real ITSCM event the Service Provider must:-
		  ○ attend Major Incident Forums as required;
		  ○ prepare event options and recommendations for consideration by the Department;
		  ○ prepare and update recovery plans;
		  ○ recover systems and services as directed by SIAM; and
		  ○ contribute to the production of a plan to return to normal operations within x days of an ITSCM event being declared

Key metrics	**Key metrics**	**Key metrics**
	▪ x% of ITSCM Plans complete • x% of ITSCM tests completed in accordance with ITSCM Test Programme	

1.6 Service Asset & Configuration

Description

Service Asset and Configuration Management (SACM) manages the service assets and Configuration Items (CIs) in order to support the other service management processes. SACM defines the service and infrastructure components and maintains accurate configuration records

Outcomes

- Improve service to customers by minimising business disruption caused by inaccurate or inadequate configuration information
- Provide accurate information on Configuration Items (CIs) and their documentation
- Enable Department to have sight of the current status and history of all defined CIs it uses
- Provide and maintain an accurate and up-to-date pictorial end-to-end view of the configuration of the Department's IT estate
- Ensure the Department reduces its use of unauthorised software
- Ensure the Department does not breach software licence terms and conditions
- Ensure the Department maximises its use of hardware assets
- Comply with the Department's Asset Management Strategy

Relationship & Interfaces

Customer/Service Consumer

- Participate in determining the level of CI granularity and relationships with the SIAM
- Participate in meetings to determining the level of Service Asset and Configuration Management integration required between SIAM and Service Providers

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Service Asset and Configuration Management Policies and Procedures.
- 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 expert trend analysis activities to the Department
- Identify potential process improvements and make appropriate recommendations to Service Providers
- Monitor and manage stakeholder compliance to the Service Asset and Configuration Management Policies and Procedures and inform Service Providers of any material non-compliance with the Service Asset Configuration Management Policies and Procedures
- Liaise with Service Provider and the Department 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

Service Provider

- Assist SIAM in the development of the Service Asset and Configuration Management Policies and Procedures
- Work with SIAM and the Department as reasonably required with the scoping of audits, impact assessments, investigation and resolution of discrepancies
- Provide the required audit data to SIAM within the required timescales and in the format specified by SIAM
- Review and comment on audit scope documents
- Monitor, analyse and report to SIAM on the accuracy of the Service Providers Configuration Management Database and provide evidence of proactive configuration management to SIAM at the Service Asset and Configuration Management Service Review meetings
- Work with SIAM and other Service Providers to assist with any Service Provider engagement and non-compliance issues
- Provide agreed configuration management measurements to SIAM
- Develop, test and implement changes to their interfaces and CI data content as defined in the interface definition documentation provided by SIAM
- Provide CI data in accordance with the interface requirements of the integrated CMDB
- Ensure that CI updates are processed in accordance with the SIAM Change Management Policies and Procedures

1.6 Service Asset & Configuration Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Update the discrepancy reports once all agreed actions have been completed • Meet with the new/enhanced project to gather project information and provide that information to Service Providers • 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 policies and procedures post project go-live • Implement and manage a single enterprise Asset Management Service. • Provide Customer access at all times to an Asset inventory repository. • 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	• Update the Service Providers own CMDB within x hours of a corresponding change being made in the live or production test estate and provide the CI data to SIAM within an additional x hours of the change being made to the Service Provider CMDB • Provide details of all change reports under which CI data updates were upon request from SIAM • Assist SIAM in determining the reason for each discrepancy, its criticality, the responsible party and actions required to address it • Review and comment to SIAM on discrepancy reports • Where requested by SIAM, provide CI data as requested or provide an explanation to the SIAM why the data cannot be provided • Agree the level of CI granularity and relationships with SIAM • Provide CI data for the new/enhanced service at the earliest opportunity following go-live • Meet with the 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 SIAM • Provide Integrator with required Asset Attributes. Such attributes include, but are not limited to: (i) Ownership (including leased Equipment); (ii) Asset type, model and release number; (iii) Estate location and physical address; (iv) Service priority and criticality rating; and (v) Contact details of any regular users.
Key metrics	**Key metrics**	**Key metrics**
	• Less than x% of Incidents, Problems and failed Changes caused by inaccurate or inadequate Service Asset and Configuration Management information • No more than x% inaccuracies identified in the Integrated CMDB	

1.7 Service Catalogue Management

Description

The purpose of Service Catalogue Management (SCM) is the development and upkeep of a Service Catalogue that contains all detail, status, possible interaction and mutual dependencies of all present services and those under development

Outcomes

- Build, maintain and manage a Service Catalogue providing the relationships between the customer facing services and the supporting services; between the IT services and the components that deliver those services and showing the relationships between the IT service catalogue and the Departments business services/processes

Relationship & Interfaces

Customer/Service Consumer

- Provide all relevant business and customer information to enable SIAM to develop and maintain the Service Catalogue
- Provide timely impact assessments to SIAM for any Service Catalogue change requests raised by Service Providers and SIAM

SIAM (Outsourced or Retained)

- Develop, maintain and distribute the Service Catalogue
- Provide on-line access to the Service Catalogue to the Department's customers
- Manage the impact assessment process for changes to the Service catalogue that are proposed by Service Providers and the Department
- Request and consolidate impact assessments from Service Providers and the Department
- Review the Service Catalogue from time to identify any errors or inaccuracies and resolve as soon as is reasonably practicable

Service Provider

- Provide all relevant information and assistance to SIAM in the development of the Service Catalogue
- Raise requests in the appropriate format to request Service Provider changes to the Service Catalogue
- Provide timely impact assessments to SIAM for any change requests raised by other Service Providers, SIAM and the Department

Key metrics

Key metrics

- Each Measurement Period, the Service Catalogue to be available to users x% of the time it should be available
- Content to be refreshed each Measurement Period as a minimum
- Data that is sourced either from the iCMDB or elsewhere to be accurately reflected in the service catalogue, following each refresh activity.
- Customer Satisfaction – Year on year improvements to the ease of use customer satisfaction rating

Key metrics

To be completed

1.8 Service Level Management

Description

The objective of the Service Level Management (SLM) process is to agree on the delivery of IT services and to make sure that the agreed level of IT service provision is attained

Outcomes

- Ensure Service Providers provide accurate Service Level management information and appropriate supporting documentation
- Undertake validation checks on Service Provider Service Level and Key Performance Indicator supporting information and raise any queries within the appropriate timescale
- Ensure that service targets are being met by Service Providers each Measurement Period
- Provide expert trending analysis and management information across all service management processes ensuring consistency and accuracy of all information provided
- Use trending analysis to identify opportunities to
    - drive through continual service improvement
    - drive down cost and improve the overall service being provided throughout the processes
    - identify opportunities to improve service and deliver business benefits in line with business priorities

Relationship & Interfaces

Customer/Service Consumer

- Review the consolidated performance summary report and provide comments where necessary to SIAM
- Chair and manage the Commercial and Performance Review meetings

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Service Level Management Policies and Procedures.
- Provide support and guidance to Service Providers in fulfilling their service level management roles and responsibilities.
- Review Service Provider management information each Service Measurement Period and produce its own expert trend analysis and management summaries to identify Service Provider performance trends and potential performance opportunities and improvements
- Identify potential process improvements and make appropriate recommendations to Service Providers
- Monitor and manage stakeholder compliance to the Service Level Management Policies and Procedures and inform Service Providers of any Service Provider material non-compliances
- 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 Department

Service Provider

- Assist SIAM in the development of the Service Level Management Policies and Procedures
- Provide management information each Service Measurement Period to SIAM in accordance with the Service Level Management Policies and Procedures
- Monitor and analyse Service Level/KPI performance and provide evidence and trend analysis to SIAM within x days of the end of each Service Management Period
- Work with SIAM 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 SIAM
- Undertake checks to ensure performance data provided to SIAM is accurate and complete
- Address and resolve any queries with the Service Measurement Period reports raised by the SIAM

Key metrics

Key metrics

- x% overall of Supplier contractual Service Levels and Key Performance Indicators reported on each Measurement Period

Key metrics

1.9 Standards & Architecture

Description

The objective of the Standards and Architecture service is to define and provide a documentation standard to which all of the Service Management Policies and Procedures will be documented. The service ensures that all Policies and Procedures are documented to this standard

Outcomes

- Defines, maintains and communicates the SIAM operational standards and acceptance criteria for each of the SIAM services
- Ensures that Policies and Procedures and other SIAM documentation is produced using the defined standard and to an acceptable quality
- Defines, maintains and communicates the technical data and technical architecture standards including technical interface requirements
- Provides an effective reference point for the Department's Project Managers to transition new or changed services in to the Departments live environment

Relationship & Interfaces

Customer/Service Consumer

- Provide impact assessment for changes to SIAM Policies and Procedures and documentation where required

SIAM (Outsourced or Retained)

- Define, make available and maintain the SIAM operational standards
- Communicate SIAM operational standards to the Service Providers
- Define, make available, maintain and communicate the technical architecture standards
- Define, maintain and communicate to the Service Providers the quality standards for all SIAM documentation
- Manage and control the impacting and quality review process for changes to all SIAM Policies and Procedures and documentation amongst the Service Providers and the Department's stakeholders
- Maintain and make available a central library of all SIAM Policies and Procedures and documentation

Service Provider

- Adhere to the SIAM Policies and Procedures and standards
- Provide impact assessment for changes to SIAM Policies and Procedures and documentation at SIAM's request

Key metrics

Key metrics

Key metrics

1.10 Financial Management Support

Description

Financial Management Support is an integrated component of service management. It provides vital information that management needs to guarantee efficient and cost-effective service delivery. If strictly implemented, financial management generates meaningful and critical data on performance

Outcomes

- Ensure Suppliers provide accurate invoices information and appropriate supporting management information documentation
- Undertake x% validation checks on Supplier invoices and raise any queries within the appropriate timescale
- Ensure charges are apportioned correctly to Department's business units where required

Relationship & Interfaces

Customer/Service Consumer

- Issue purchase order numbers to Service Providers for inclusion on their invoices
- Confirm with the Service Providers any man day effort chargeable prior to the Service Providers issuing appropriate invoices
- Determine, provide and maintain the the Department's Apportionment Model
- Pay valid Service Providers invoices within the terms of the contract

SIAM (Outsourced or Retained)

- Define, make available, maintain and communicate the Financial Management Policies and Procedures.
- Provide support and guidance to Service Providers in fulfilling their financial management roles and responsibilities
- 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 the invoices, supporting MI and the contract value for the service provided and reject any invalid invoices back to the Service Provider
- Engage fully with Service Providers to resolve any invoice discrepancies
- Provide a report of its findings in the review of Service Provider invoices to the Department
- Provide a consolidated statement of charges incurred by the Department each Service Measurement Period supported by invoices and MI provided by Service Providers detailing the consumption of products and services by the Department
- Provide reports to the Department providing recommendations on the apportionment of charges to the Department's Business Units based on the Department's Apportionment Model
- Identify potential process improvements, make appropriate recommendations to Service Provider and co-ordinate improvement activities that span multiple Service Provider
- Monitor and manage stakeholder compliance to the Financial Management Policies and Procedures and inform Service Providers of any Service Provider material non-compliances

Service Provider

- Assist the Service Integrator in the development of the Financial Management Policies and Procedures
- Raise invoices (including service credits) and associated supporting management information for products and service provided in accordance with the Service Provider contract terms and conditions
- Engage with SIAM to resolve invoice discrepancies
- Refund incorrect payments as soon as possible
- Work with SIAM and other Service Providers to assist with any engagement and non-compliance issues

Key metrics

Key metrics

- x% of invoices accurately presented and validated
- x% of charges apportioned correctly to the Department's business units

Key metrics

1.11 Service Provider Management

Description

Service Provider Management manages Service Providers and the services they provide, it is aimed at securing consistent quality at the right price

Outcomes

- Effective and robust processes in place to manage the on-boarding of Service Providers to the Service Management processes
- Facilitate and ensure the rapid migration of Service Providers to the Service Management processes and procedures
- Ensure that Service Providers have in place and maintain robust Exit Management Plans

Relationship & Interfaces

Customer/Service Consumer

- Agree with SIAM the Service Provider categorisation
- Notify SIAM of the Service Provider lead contact to interface with the SIAM for on-boarding activity
- Agree sign-off that on-boarding has been complete
- Review and approve Service Provider Exit Plans (including SIAM Tower Exit Plans) for accuracy and robustness
- Attend and observe tests of Service Provider and SIAM Tower Exit Management Plans;
- Work with SIAM to identify, agree & undertake periodic audits of Exit Management Plans and

SIAM (Outsourced or Retained)

- Hold an introductory meeting with new Service Providers to provide an overview of the services provided by SIAM and to provide any clarification on SIAM's Policies, Procedures and Standards
- Ensure resource is allocated to the new Service Provider to manage the take-on
- Develop a plan for the take-on of the new Service Provider, hold regular meetings with the Service Provider and report on Service Provider engagement and progress against the plan towards on-boarding throughout the take-on process
- Provide sign-off that the Service Provider has been successfully on-boarded to the SIAM Policies, Procedures and Standards when it is complete
- Review Service Provider's Exit Management Plans to ensure their accuracy and robustness
- Perform and manage tests of Service Provider's Exit Management Plans in accordance with the agreed Exit Management Test Programme

Service Provider

- Discuss with SIAM operational leads which service management processes are applicable to the Service Provider based on their contractual obligations
- Identify any gaps in compliance with SIAM's policies and procedures and agree a plan to achieve compliance
- Meet regularly with SIAM throughout the take-on progress to review progress towards compliancy
- Agree sign-off that on-boarding has been complete
- Work with the SIAM and the Department as reasonably requested with the scoping of Exit Management Plan audits, impact assessments, investigation and resolution of discrepancies;
- Provide the required Exit Management audit data to SIAM within the required timescales and in the format specified

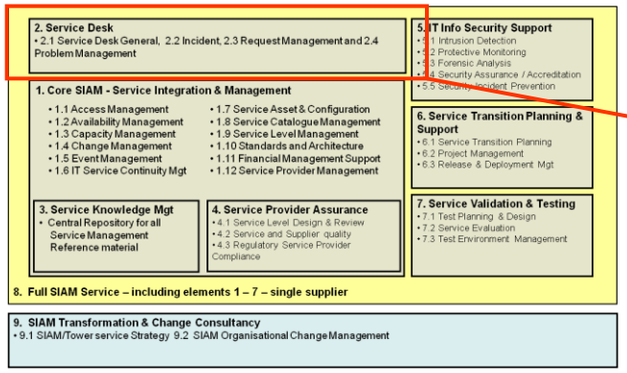
Key metrics

Key metrics

- % of Suppliers to have Exit Management Plans in place, measured every x months
- Reduce the time taken to take-on Suppliers year on year

Key metrics

2. Service Desk



2. Service Desk
2.1 Service Desk General, 2.2 Incident, 2.3 Request Management
2.4 Problem Management, 2.5 Access Management

Description

Service Desk acts as the single point of contact for users and IT Service Management. The Service Desk manages all Incidents and Service Requests and its primary purpose is to restore normal service operation to all users as quickly as possible e.g. by resolving a technical issue, fulfilling a Service Requests or answering a technical query.

The Service Desk includes the following functions:-

- **2.1 Service Desk (General)**
  - Acts as the single point of contact for all the Department's users
- **2.2 Incident Management**
  - Level 1 Support – 1st level support, resolving incidents at first point of contact using case bases provided by the Service Providers or Departments;
  - Level 2 and 3 Integration – Provides an effective quality interface to level 2 and 3 support ensuring incidents that are not resolved at first point of contact are accurately captured, classified and assigned to the appropriate level 2 and level 3 Service Provider expert domains;
- **2.3 Request Management**
  - Ensures that Service Requests that are submitted by the Department's users are accurately captured, classified and assigned to the appropriate Service Provider(s) for fulfilment;
- **2.4 Problem Management**
  - For incidents that cannot be prevented, the Service Desk provides an effective quality interface to the appropriate level 2 and level 3 Service Providers to determine the underlying cause and initiate and track action to remove the error.
- **2.5 Access Management**
  - Ensures the organisation is able to maintain the confidentiality of it's information effectively.
  - Users have the level of access to execute their jobs effectively.
  - The ability to audit use of services and to trace the abuse of services
  - The ability to easily revoke access rights when needed.

2.1 Service Desk (General)

Description

Acts as the single point of contact for all the Department's users

Outcomes

- Improve customer service, perception and satisfaction year on year
- Answer calls to the Service Desk within the required timescales during the required service hours
- Reduce call abandonment rate
- Proactively monitor other Supplier's information e.g. web sites, bulletin boards etc to capture and provide information on Incidents, Problems, Known Errors and Workarounds and publish details of that information to the Department's users
- Provide the capability for users to report incidents to the Service Desk by automated means
- Reduce the amount of service disruption by providing and maintaining accurate management information from integrated processes, including but not limited to: Casebase, workaround and Service Asset and Configuration Management information across all Service Management

Relationship & Interfaces

Customer/Service Consumer

- Provide all the necessary information when contacting the Service Desk to report incidents or raise service requests
- Ensure all relevant information is provided by users when contacting the Service Desk
- Participate in the Service Desk customer satisfaction surveys as requested by SIAM

SIAM (Outsourced or Retained)

- Define the Service Desk procedures.
- Provide a Service Desk function which acts as a single point of contact for users and suppliers to report incidents and raise service requests.
- Handle each contact between the user and the Service Desk in a professional, efficient and service-oriented manner
- Handle each contact between the Service Provider and the Service Desk in a professional, efficient and service-oriented manner
- Ensure that Service Desk agents are certified in accordance with the standards and processes used by SIAM
- Develop a customer satisfaction survey to gather the views and feedback from users on the service provided by the Service Desk
- Conduct a customer satisfaction survey every Service Management Period
- Provide and report to the Department the results of the customer satisfaction survey each Measurement Period

Service Provider

- Ensure all relevant information is provided to the Service Desk when contacts are made
- Provide information of Case Bases and Knowledge Articles to SIAM to enable it to update the Service Desk scripts
- Regularly review and update Case Bases and Workarounds to ensure the currency of information contained in them and provide such information to the Service Desk

Key metrics

Key metrics

• Service Desk to be available to receive incidents, service requests and change requests % of the time it is contracted to be available
• Each Measurement Period to answer % of calls offered to the Service Desk within N seconds
• To ensure the call abandonment rate does not exceed % in each Measurement Period
• Each Measurement Period to respond to % of web-based requests within N hours of the request being made
• Level of customer satisfaction related to the services provided by the Service Desk to improve year on year as follows:-

Key metrics

•% of Incidents passed that could have been resolved by the Service Desk using an available Knowledge Article.

2.2 Incident Management

Description

Level 1 Support – 1st level support, resolving incidents at first point of contact using case bases provided by Service Providers.

Level 2 and 3 Integration – Provides an effective quality interface to level 2 and 3 support ensuring incidents that are not resolved at first point of contact are accurately captured, classified and assigned to the appropriate level 2 and level 3 Service Provider expert domains.

Outcomes

•Improve the management, co-ordination and turnaround of incidents

•Accurately categorise the severity of Incidents reported by users

•Improve service availability by assigning incidents received from customers to the appropriate Service Provider first time

•Improve service availability and reduce end to end incident resolution times by improving first contact resolution year on year

•Improve service availability of IT and the number of Business Days lost by reducing the number and severity of Incidents reported to SIAM by a percentage year on year

•Improve service to customers by minimising business disruption caused by Incidents

•Improve the overall unmitigated end to end Incident resolution times year on year

Relationship & Interfaces

Customer/Service Consumer

•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

SIAM (Outsourced or Retained)

- Define, make available and maintain the Incident Management Policies and Procedures.
- Communicate the Incident Management Policies and Procedures to the Service Providers and the Department.
- Provide support and guidance to the Department and its 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 Policies and Procedures by:-
  - leading and managing the Major Incident Resolution forum with the Department and appropriate Service Providers for all Severity 1 incidents
- 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 on the incident management system
- Allocate incident severity levels for all incidents and faults reported to the Service Desk
- Assign correctly reported incidents to the appropriate Service Provider resolver group
- Provide incident updates to users when requested

Service Provider

- Provide details of the Service Providers support organisation and contacts points to SIAM to enable the 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 Department
- 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 Incident Management system
- Allocate incident severities in accordance with the Incident Severity definitions contained in the Incident Management Policies and Procedures
- Provide updates on the progress of incidents when requested to do so by the Service Desk

2.2 Incident Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Make every effort to provide incident resolution confirmation	• 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	• Inform the Service Desk when an incident has been resolved and provide a valid resolution code – Perform incident diagnosis on all incidents assigned to the Service Provider
Key metrics	**Key metrics**	**Key metrics**
	• Each Measurement Period to resolve % of incidents received at first point of contact • To assign % of incidents to the appropriate Supplier on first contact each Measurement Period • To assign incidents to the correct Supplier Resolver Group within set times for each Severity • % of Incidents assigned to SIAM in each Measurement Period for resolution that are resolved within the required timescale for that Incident Severity • % year on year reduction for each Severity in the number of incidents reported to SIAM • % of incidents resolved and closed each Measurement Period within a predefined amount of days., decreasing year on year throughout the contract. • Incident Re-open rate – No more than % of incidents that have been “resolved” to be re-opened within 1 week of resolution	• Same set of metrics as prescribed for the Service Integrator.

2.3 Request Management

Description	Outcomes
Ensures Service Requests that are submitted by users are accurately captured, classified and assigned to the appropriate Service Provider(s) for fulfilment;	•Improve the management, co-ordination and turnaround of both customer requests and service requests •Improve service availability by assigning service requests received from customers to the appropriate Service Provider first time

Relationship & Interfaces

Customer/Service Consumer

- 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

SIAM (Outsourced or Retained)

- Define, make available and maintain the Service Request Management Policies and Procedures.
- Communicate the Service Request Management Policies and Procedures to the Service Providers and the Department.
- Provide support and guidance to the Department and its 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 its own expert trend analysis and management summaries to identify trends or significant changes or increases in service request volumes, for discussion with the Department and the Service Providers
- Identify potential process improvements and make appropriate recommendations to Service Providers and the Department
- Monitor and manage stakeholder compliance to the Service Request Management Policies and Procedures

Service Provider

- Provide details of the Service Providers support organisation and contacts points to SIAM to enable the accurate assignment of service requests by the Service Desk
- Accept and acknowledge service requests that are correctly assigned by the Service Desk
- 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 each Service Management Period to the appropriate Service Request Forums in accordance with the Service Request Management Policies and Procedures

2.3 Request Management

……Continued

Relationship & Interfaces		
Customer/Service Consumer	**SIAM (Outsourced or Retained)**	**Service Provider**
	• Inform Service Providers of any Service Provider material non-compliance with the Service Request Management Policies and Procedures • Engage with Service Desk, Service Providers and the Department staff as appropriate where there are issues and problems with the processing of service requests • Ensure that service requests are expedited timeously 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 requests submitted by users • Ensure that all requests submitted are recorded on the request management system	
Key metrics	**Key metrics**	**Key metrics**
	• Each Measurement Period, % of all requests to be assigned to the appropriate Supplier with the required time timeframe	

2.4 Problem Management

Description	Outcomes
For incidents that cannot be prevented, the Service Desk provides an effective quality interface to the appropriate level 2 and level 3 Service Providers to determine the underlying cause and initiate and track action to remove the error.	• Improve service availability of IT and Business impact by reducing the number and severity of Problems reported to SIAM by a percentage year on year • Improve service to customers by minimising business disruption caused by Problems • Improve the overall unmitigated end to end Problem resolution times year on year

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• 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 • Formally sign-off all solution approvals • Formally sign-off all Problem/Known Error closures	• Define, make available and maintain the Problem Management Policies and Procedures. • Communicate the Problem Management Policies and Procedures to the Service Providers and the Department. • Provide support and guidance to the Department and its Service Providers in fulfilling their problem management roles and responsibilities. • Log Problems in accordance with the Problem Management Policies and Procedures • Identify, prioritise and assist to manage through to resolution those Problems that cause or have the potential to cause business disruption • Assign Problems to the appropriate Service Provider resolver group • Coordinate Problem Management activities which span multiple Service Providers • Receive Problems for external assignment from Service Provider and assign them to the appropriate Service Provider	• Identify potential Problems and raise with SIAM • Submit fully documented and validated Problem records to SIAM using the standard Problem template • Classify Problems using a Problem Severity Model • Log and track Problems during their lifecycle on the Service Providers Problem Management System • Accept and resolve Problems when they are correctly assigned to the Service Provider • Acknowledge correctly assigned Problems within the required timescales • Inform SIAM of any Problems that have been incorrectly assigned to them

2.4 Problem Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Ensure Service Providers conduct Root Cause Analysis on any Problems raised and the Problem record is updated accordingly to reflect the analysis • Review Service Provider management information on a monthly basis and produce its own expert trend analysis and management summaries to identify trends or significant changes or increases in Problem volumes for discussion with the Department and the Service Provider at the appropriate forums • Proactively monitor Problem volumes • Collate, maintain and publish to the Department accurate and up to date information on Problems, Workarounds and Known Errors • Monitor and report to the Department on the 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 Department	• Provide progress updates on Problems in a timely manner to SIAM 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 SIAM to prevent repetitive issues • Continually evaluate the linked incident count to Known Errors and Problems to ensure the business impact is current
Key metrics	**Key metrics**	**Key metrics**
	•Better than n:n ratio of number of Problem records closed in each Measurement Period compared against number of Problems opened in the same period •Ratio of new Incidents that linked to Problems and Known Errors in a Measurement Period compared to total Incidents linked to the same Problem/Known Error at the end of the Measurement Period •At least % of Problems records closed as a result of a deployed change each Measurement Period •Less than % of fixes deployed to Problems that result in future Incidents	

2.5 Access Management

Description

Access management is the process of granting authorised users the right to use a service and helps to protect the confidentiality, integrity and availability of assets and information

Outcomes

- Ensures the organisation is able to maintain the confidentiality of it's information effectively.
- Users have the level of access to execute their jobs effectively.
- The ability to audit use of services and to trace the abuse of services
- The ability to easily revoke access rights when needed.

Relationship & Interfaces

Customer/Service Consumer

- Issue requests for user access to SIAM 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

SIAM (Outsourced or Retained)

- Provide access to systems as requested by users
- Reject any request that has not been properly approved in accordance with the approval process
- Undertake periodic audits to ensure correct user access has been provided to systems
- Inform the Department where it suspects inappropriate user access has been requested

Service Provider

- Inform SIAM where it suspects inappropriate user access has been granted e.g. where the Service Provider suspects inappropriate access is granted during its investigation of an incident

Key metrics

- Not Applicable

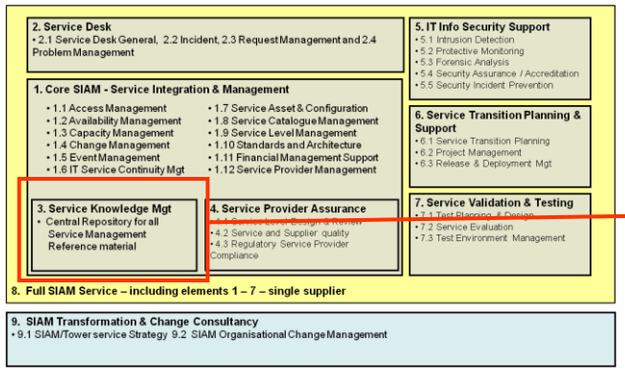
Key metrics

•Percentage of user requests fulfilled on time and in line with the Service Target
•Percentage of users with incorrect system access found as a result of audit activity

Key metrics

Not Applicable

3. Service Knowledge Management



3. Service Knowledge Mgt

- Central Repository for all Service Management Reference material

Description

Service Knowledge Management provides central repository for all Service management reference material. Service Knowledge Management feeds into the Service Desk and enables a Department to improve the quality of management decision making by ensuring that reliable, current, historic and secure information and data is available throughout the service lifecycle

3. Service Knowledge Management

Description

Provides central repository for all Service management reference material. Service Knowledge Management feeds into the Service Desk and enables a Department to improve the quality of management decision making by ensuring that reliable, current, historic and secure information and data is available throughout the service lifecycle

Outcomes

- Improvements made throughout the service management processes and disciplines by having all of the essential and required information in one place to enable better management decisions to be made
- Essential information is kept up to date and is consistent at all times and readily available to those who require it
- Allocates overall accountability for defining and maintaining a holistic Knowledge Management Strategy, ensuring that SIAM Communications and Strategy & Architecture accountabilities integrate with this

Relationship & Interfaces

Customer/Service Consumer

- Ensure that all relevant business information is made available to SIAM to enable the development of the Service Knowledge Management repository

SIAM (Outsourced or Retained)

- Define and maintain the Knowledge Management Strategy
- Establish and maintain Knowledge Management interfaces and transfer mechanisms
- Establish and maintain data requirements
- Establish data & information management procedures
- Develop the central database for Knowledge Management
- Make the Service Knowledge Management information available and accessible to all interested parties
- Capture, store, analyse and share data effectively across lifecycle processes and Service Providers

Service Provider

- Ensure that all relevant Service Provider information is made available to SIAM to enable the development of the Service Knowledge Management repository

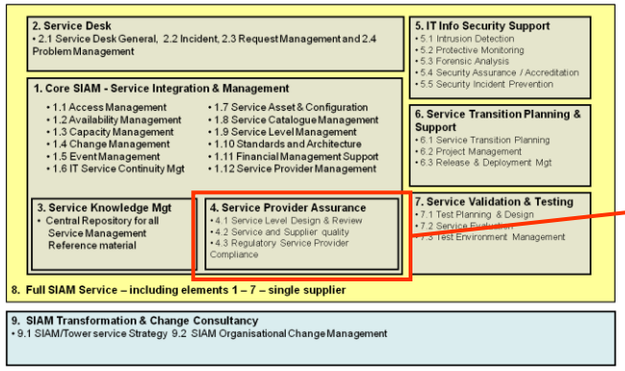
Key metrics

Key metrics

- Accuracy of the Service Knowledge Management repository

Key metrics

4. Service Provider Assurance



4. Service Provider Assurance
- 4.1 Service Level Design & Review
- 4.2 Service and Supplier quality
- 4.3 Regulatory Service Provider Compliance

Description

This ensures that Service Providers agree on the delivery of all end-to-end IT Services and to make sure that the agreed level of IT Service provision is attained. Service Performance Assurance functions are:

• 4.1 Service Level Design & Review – ensuring end-to-end service levels to meet business/departmental needs, and are regularly reviewed to maintain alignment with Business priorities

• 4.2 Service and Service Provider Quality – providing expert trending analysis and management information across all service management processes ensuring consistency and accuracy of the information provided – using trend analysis to:

- Identify opportunities to drive through continual service improvement and inform future service level design
- Drive down cost & improve the overall service being provided throughout the processes
- Identify opportunities to improve service to deliver business/departmental benefits in line with business/departmental priorities

• 4.3 Regulatory Service Provider compliance – monitors and manages Service Provider compliance to the Service Management Policies and Procedures ensuring that non-compliances are raised and managed through to resolution.

4.1 Service Level Design & Review

Description	Outcomes
Ensuring end-to-end service levels to meet business/departmental needs, and are regularly reviewed to maintain alignment with Business priorities	• Service Levels, Service Targets and Key Performance Indicators compliment and contribute to the achievement of Departmental business objectives and targets • Service Levels, Service Targets and Key Performance Indicators have clear relationships with Departmental business objectives and targets • Service Levels, Service Targets and Key Performance Indicators are clear and unambiguous and clearly articulate their intent

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Provide details of the Department's business objectives and targets to SIAM and ensure SIAM have a full understanding of those business objectives and targets • Review and provide comment/sign-off of proposed Service Levels, Service Targets and Key Performance Indicators to ensure alignment with the Department's business objectives	• Engage with the Department to understand the Department's business objectives and targets to ensure alignment with the end-to-end Service Levels, Service Targets and KPIs • Provide expert input to periodic Service Level, Service Target and KPI audit reviews as and when required • Fully define new or amended end-to-end Service Levels, Service Targets and KPI requirements • Review and agree the timescales for the implementation and activation of Service Levels, Service Targets and KPIs	• Provide input to periodic Service Level management audit reviews when required • Assist SIAM and the Department in the definition of the Service Levels, Service Targets and KPIs • Fully define new or amended Service Levels, Service Targets and KPIs requirements • Confirm the service level management impact arising from new or amended Service Levels, Service Targets and KPIs requirements and submit to the SIAM for approval • Propose a timetable for the implementation and activation of new/amended Service Levels, Service Targets and KPIs
Key metrics	**Key metrics**	**Key metrics**
	•% of Service Levels, Service Targets and Key Performance Indicators fully compliment Departmental business objectives and targets •% of Service Levels, Service Targets and Key Performance Indicators are in place and signed off for measurement prior to the Service going live	

4.2 Service & Service Provider Quality

Description	Outcomes
Providing expert trending analysis and management information across all service management processes ensuring consistency and accuracy of the information provided	• Identify at least 3 service improvement initiatives from expert trending each Measurement Period • Ensure that service improvement initiatives are linked to and achieve cost reduction and/or business benefits for the Department

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Review service improvements provided by SIAM • Approve service improvements where required	• Gather and provide expert analysis of the end-to-end performance using analytical tools and processes • Fully understand the Department's business objectives and targets • Develop a standard template for service improvement proposals • Develop service improvement proposals to support cost reductions and business benefits and submit to the Department	
Key metrics	**Key metrics**	**Key metrics**
	• Number of service improvement initiatives proposed by SIAM	

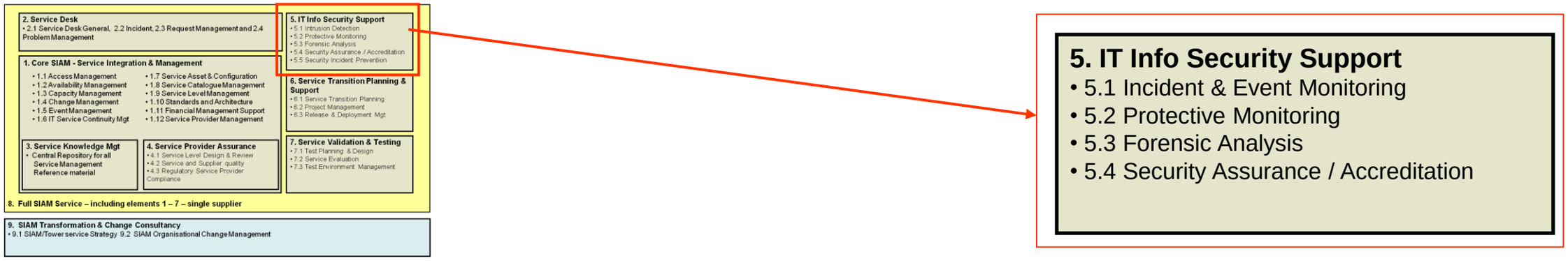
4.3 Regulatory Service Provider Compliance

Description	Outcomes
Monitors and manages Service Provider compliance to the Service Management Policies and Procedures ensuring that non-compliances are raised and managed through to resolution.	• Less than % contractual Service Provider non-compliances raised during each Measurement Period • No Service Provider non-compliances to remain open for more than 2 Service Measurement Period

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Inform SIAM of any issues encountered that the customer believes may be a Service Provider non-compliance	• Monitor and manage stakeholder compliance to the Service Management Policies and Procedures • Arrange and manage Service Provider compliance management meetings • Inform Service Providers of any Service Provider material non-compliance with the Service Management Policies and Procedures • Ensure remedial action plans that are put in place by Service Providers to resolve non-compliances are actively managed through to successful completion	• Comply with the Service Management Policies and Procedures • Attend Service Provider compliance management meetings where required by SIAM • Put in place and manage remedial action plans to resolve non-compliances • Work with the SIAM, the Department and other Service Providers to assist with any Service Provider engagement and non-compliance issues
Key metrics	**Key metrics**	**Key metrics**

5. IT Information Security Support



5. IT Info Security Support
- 5.1 Incident & Event Monitoring
- 5.2 Protective Monitoring
- 5.3 Forensic Analysis
- 5.4 Security Assurance / Accreditation

Description

IT Information Security Support aligns Information Security Management requirements with business/departmental security ensuring effective Information Security Management across all Service Providers and service management operations. It creates security policies, standards and procedures and manages the information security requirements of the end-to-end service. The functions are:-

- 5.1 Incident & Event Monitoring – provides the full security Event and Incident management service including incident identification, logging, tracking, investigation and resolution, security help and advice
- 5.2 Protective Monitoring – provides proactive protection of the Departments IT systems including threat monitoring, Health Check / Penetration Testing, security scanning and the operation of technical security controls.
- 5.3 Forensic Analysis – produce Forensic Readiness plans and asset interrogation and evidential reporting capability
- 5.4 Security Assurance and Accreditation – provides end-to-end assurance and accreditation including security audit, vulnerability identification, assessment and management, security risk and compliance management

5.1 Incident & Event Management

Description

Provides the full security Event and Incident management service including incident identification, logging, tracking, investigation and resolution, security help and advice

Outcomes

- Ensures that Security events and incidents are detected, logged, contained and managed through to resolution
- Provides help and advice on all security matters

Relationship & Interfaces

Customer/Service Consumer

- Review service improvements provided by SIAM
- Approve service improvements where required

SIAM (Outsourced or Retained)

- Log, consolidate and analyse activity on agreed devices on the Department's estate and at the perimeter to identify in real time any anomaly that might constitute a Security Event
- Ensure events identified as potential Security Incidents are adequately investigated by the relevant Service Provider and recorded and tracked as a Security Incident
- In all cases ensure where a risk is identified the Service Providers take remedial action as necessary and agreed with the Department - including where appropriate co-ordinating the activities of the Service Providers involved
- Provide a security incident reporting, investigation and management service supported by appropriate contact facilities and tooling and communicate the process to all stakeholders
- Receive and record all security events, incidents and breaches of Security Policies, Security Standards and Security Procedures reported in accordance with the Security Incident Guide or received via other authoritative sources
- Ensure that data on incidents is sufficiently comprehensive, granular, accessible and can be readily interrogated to inform decisions on controls
- Provide support to Service Providers and the Department in identifying and handling Security Incidents by increasing awareness
- Ensure that any Security Incident that constitutes a risk to the Department is fed into the Risk Management process
- Take the necessary steps to contain the incident and conduct an investigation to establish its nature and take all necessary action to resolve the incident
- Use information from the database intelligently to inform the overall security, vulnerability and risk posture of the Department
- Undertake trend analysis and reports on queries raised to inform future training and the need for Bulletins and/or notices that should be published by SIAM
- Continuously monitor the Department's employees and agents' use of the Internet, taking into account any relevant information from Service Providers
- Provide details to the Department of any successful or attempted access to prohibited internet content

Service Provider

Key metrics

Key metrics

- Number of service improvement initiatives proposed by SIAM

Key metrics

5.2 Protective Monitoring

Description

Provides proactive protection of the Departments IT systems including threat monitoring, Health Check / Penetration Testing, security scanning and the operation of technical security controls

Outcomes

- Ensures the correct level of protection is provided on the Departments IT systems
- Ensures the Department's IT systems can identify and are protected from security threats
- Ensures the appropriate level of security monitoring is provided to the Departments IT estate
- Ensures that protective monitoring of ICT systems aligns with HMG Good Practice Guide 13 (GPG13)

Relationship & Interfaces

Customer/Service Consumer

- Assist SIAM where necessary in its definition of the Layered Security Strategy

SIAM (Outsourced or Retained)

- Develop a Layered Security Strategy appropriate to the protection of the Department's IT estate (including the services delivered to the Department by the Service Providers) and assets (including the Department's Information Assets) to be refreshed annually/continuously updated to reflect the evolving threat landscape
- Monitor and review the availability of Anti-Virus updates and Security Releases and inform Service Providers and the Department of their relevance
- Monitor the access of the Department and Service Providers staff to the Department's data and particularly those with privileged user credentials
- Conduct regular scans (monthly) of nominated IT Services to identify the number and location of Dormant secondary IDs in circulation and report to the Department
- Review Service Providers mechanisms and controls for allowing access to the Department's information assets and services to assure their alignment with the Security Policies, Standards and processes
- Provide a Security Scanning Service to check the configuration of all servers hosted and managed by the Service Providers that provide services to the Department
- Perform the scheduled scans and provide a quarterly written report of deficiencies discovered that could expose the server and/or the infrastructure to a security risk
- Produce best practice guidance around when and how IT Health Checks and Penetration Tests should be undertaken
- Propose and deliver a schedule of Penetration Tests to assure key services and infrastructure components on a regular basis
- Assure the scope of any proposed IT Health Check and Penetration Test activity in support of accreditation/re-accreditation
- Co-ordinate Service Providers action to enable the execution of perform IT Health Check and/or Penetration Tests
- Review findings of all perform IT Health Check and/or Penetration Tests to check the compliance of Service Providers products and services against Security Policies, Standards, Processes and Security Management Plans and report to the Department of their criticality, including making recommendations to deal with them

Service Provider

- Adhere to the Department's Layered Security Strategy
- Monitor, review and apply all necessary Anti Virus updates as applicable
- Assist SIAM in forensic investigations
- Monitor the access of the and Service Providers staff to the Department's data

5.2 Protective Monitoring

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Provide technical and operational configuration of Firewalls to the Service Providers and inform of any changes • Inform the Department of any Service Provider failure to operate the Firewalls for which they are responsible in accordance with the notified configuration and/or the Security Policies, advise the Service Provider of action to take and track to completion • Provide, on request, information to the Service Providers on the process to be followed to generate audit trails pursuant to the Security Policies, Security Standards and Security Procedures • Review audit trails and notify the Department of any anomalous activity identified by SIAM or notified to SIAM by the Service Provider • Monitor and review alignment to HMG Good Practice Guide 13 (GPG13)	
Key metrics	**Key metrics**	**Key metrics**
•TBC	•TBC	•TBC

5.3 Forensic Analysis

Description

Produce Forensic Readiness plans and asset interrogation and evidential reporting capability.

Outcomes

- Defines the strategy for forensic analysis for the Department's IT systems
- Ensures that processes are in place for detailed analysis of the Department's IT assets

Relationship & Interfaces

Customer/Service Consumer

- Assist SIAM in forensic investigations where appropriate

SIAM (Outsourced or Retained)

- Produce a Forensic Readiness plan and Forensic Readiness process to facilitate forensics activity, including the provision of advice and guidance, coordination of activities and liaison with relevant organisations
- Where a Security Event has occurred, unless otherwise authorised by the Department, take the necessary action to preserve evidence including, where appropriate, formal seizure and quarantining of any assets involved
- Advise the Department on the scope of any forensic examination it wishes to take of any hardware
- Represent the Department at any legal proceedings where required

Service Provider

- Assist SIAM in forensic investigations where appropriate

Key metrics

•TBC

Key metrics

- TBC

Key metrics

•TBC

5.4 Security Assurance & Accreditation

Description

End-to-end assurance and accreditation including security audit, vulnerability identification, assessment and management, security risk and compliance management

Outcomes

- Ensures the Department Security Policies, Security Standards and Procedures are continually aligned to HMG Security Policies and Standards and are up to date at all times
- Ensures all Service Providers and the Department's staff are aware of their responsibilities in respect of IT Information Security & IA specialists in role of CESG Accreditor role are certified
- Ensures the Department's Projects are assessed and have appropriate security accreditation
- Ensures security risks are known, minimised and managed accordingly
- Assures and ensures Service Providers compliance to Security Policies, Security Standards and Security Procedures
- Defines a Department Security strategy that has security control at the correct levels and layers

Relationship & Interfaces

Customer/Service Consumer

- Adhere to the Security Policies, Security Standards and Security Procedures
- Review the Security Policies, Security Standards and Security Procedures and provide comments to SIAM
- Approve any changes to the Security Policies, Security Standards and Security Procedures
- Provide all necessary Project information and assistance required by SIAM to support the security accreditation process
- Review and comment on risk assessments and reports provided by SIAM
- Ensure risk owners are identified for all security risks raised by SIAM
- Provide all necessary business information and assistance required by SIAM to support the security audit process and schedule
- Review and comment on the Annual Statement of Control and Vulnerability provided by SIAM
- Attend Security Awareness sessions and workshops and other specialist security meetings organised by SIAM where required

SIAM (Outsourced or Retained)

- Keep abreast of changes in HMG Security Policies and Security Standards that have relevance for the Department and maintain comprehensive knowledge of influences on the Department's security stance by reference to nominated including but not limited to HMG SPF & HMG IA Standard nos. 1 & 2
- Create, interpret, revise, maintain and communicate the Department's Security Policies, Security Standards and Procedures as required
- Review Security Policies, Security Standards and Procedures at least annually in light of evolving standards, the Department's IT and related Strategies, Service Provider views and Industry Best Practice
- Identify, recommend and impact and communicate changes required to Security Policies, Security Standards and Procedures and update accordingly when agreed with the Department to Service Providers and other stakeholders as agreed
- Define, manage and communicate the end-to-end Security Accreditation process
- 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 Department
- Maintain accreditation status
- Pro-actively monitor and progress completion of all required accreditation documentation and resolution of Security issues, including reporting and escalation to the Department as required
- Monitor, investigate and assess the cumulative effect on the Department's business of all IT security risks reported from agreed sources, on the Estate
- Advise the Department 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 Department's policies on make recommendations to the Department regarding the acceptability of the risks identified
- Act as the Department's agent in providing, withholding or qualifying consent on behalf of the Department where a Service Provider requires authorisation before embarking on a course of action in connection with the provision of security services

Service Provider

- Adhere to the Security Policies, Security Standards and Security Procedures
- Review the Security Policies, Security Standards and Security Procedures and provide comments to SIAM
- Provide all necessary information and assistance required by SIAM to support the security accreditation process
- Put in place and actively manage remedial actions to resolve any issues discovered by SIAM in its accreditation assessment
- Actively monitor and minimise security risks known to the Service Provider or highlighted to the Service Provider by SIAM
- Assist SIAM in Security Audits by providing all necessary information, data and resource to enable SIAM to perform its audits
- Put in place and actively manage remedial actions to resolve any issues discovered by SIAM as part of its audit activity
- Attend Security Awareness sessions and workshops and other specialist security meetings organised by SIAM where required

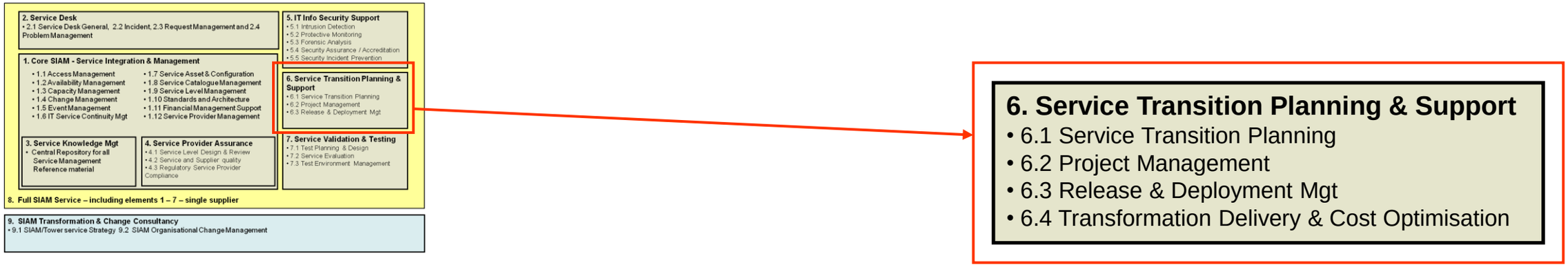
5.4 Security Assurance & Accreditation

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Act as a central point for the receipt of requests from the Department 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 Department from time-to-time to assist in the investigation of a user • Monitor Service Provider compliance with the Department's Security Policies, Standards and Processes and advise Service Providers of the action required to resolve the non-compliances and monitor progress toward completion of the recommendations within a timeframe agreed with the Department • Develop, maintain and undertake a programme of Security audits to provide appropriate assurance of Service Providers compliance with the Department'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 Department and Service Provider staff • Develop and maintain appropriate supporting material (e.g. presentations, intranet inserts, posters and leaflets), consistent with any Department internal awareness programme and strategy and undertake Security Awareness as agreed with the Service Provider • Develop a communications plan to effectively exploit the Departments internal communications tools as a means of publicising changes to Security Policies, Security Standards and Security Procedures and of notifying other information that may reasonably be required by the Department to be posted	
Key metrics	**Key metrics**	**Key metrics**
•TBC	•TBC	•TBC

6. Service Transition Planning & Support



Description

Service Transition Planning and Support manages the planning, delivery and transition of IT projects from Project teams and IT developers in to live operations by ensuring Projects deliver services designed for successful operational delivery of Department's business requirements and deliver operable and economically sustainable maintainable solutions.

Service Transition feeds into the Core SIAM Service Integration and Management in terms of Change Management (Change Evaluation & Post Implementation Review). Service Transition Planning and Support consists of the following functions:-

- 6.1 Service Transition Planning – planning service transition, impact analysis with recovery/back up and back out plans

- 6.2 Project Management – methodologies to ensure robust, risk mitigated management of service transitions from development into live environments

- 6.3 Release and Deployment – ensures releases are deployed in to the Production Environment in order to deliver value to client Department and be able to hand over service to operations
- 6.4 Transformation Delivery & Cost Optimisation – ensures cost optimisation is driven through by SIAM during transformation & into run rate operation

6.1 Service Transition Planning

Description

Planning service transition, impact analysis with recovery/back up and back out plans

Outcomes

- Owns and ensures the smooth and effective transition of Projects in to the live environment including the handover to the Department's live operations
- Provides oversight, leadership and integration of Transition activities across all stakeholders
- Manages the planning, design, delivery and support of operational environments used by IT Projects for transition and production processing
- Provides knowledge based assessment of transition and operational costs, issues and risks for input at all stages of the project lifecycle
- Ensures incidents and service disruption are minimised when Projects go live

Relationship & Interfaces

Customer/Service Consumer

- Review and approve the plan to deliver service transition
- Maintain the overall project plan that will incorporate 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

SIAM (Outsourced or Retained)

- Define, make available and maintain the Service Transition Planning and Support Policies and Procedures
- Communicate the Service Transition Planning and Support Policies and Procedures to the Service Providers and the Department.
- Engage with Service Providers and the Department Project staff throughout the project transition 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 to the Department of progress against the plan
- 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 Department and operational Service Providers

Service Provider

- Review and approve the plan to deliver service transition
- Complete all activities in the service transition delivery plan that are assigned to the Service Provider

Key metrics

Key metrics

•Less than x% of incidents reported in the first 3 months following go-live that are directly attributable to non-functional requirement failures

•Baselined Transition delivery plans established within x weeks of initial engagement for x% of Projects

•Reduce the average cost of Transition Planning support to Projects by x% year on year

Key metrics

6.2 Project Management

Description	Outcomes
Methodologies to ensure robust, risk mitigated management of service transitions from development into live environments	• Manages the planning and delivery of IT Projects from Project Teams and IT operators to live operations • Ensures and demonstrates that Project plans and milestones within those plans are met • Ensures Project risks are effectively and efficiently managed • Ensures accuracy in the estimates made in the number of days specified on Project Service Requests and therefore manages costs • Demonstrates reductions in costs to the Departments through increased re-use of resources • Demonstrates a reduction in the number of IT Projects that are implemented with non-standard IT services/components

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Identify projects for project engagement and provide the project assignment brief for review and comment by SIAM • Ensure commercial cover is provided for the project • Review and agree the project assignment brief response including the estimates • Provide input to the post implementation report and sign-off • Provide the Department project list to SIAM	• Ensure suitable resources are allocated as part of the engagement process • Review and confirm acceptance of the project assignment brief and provide a response to the project assignment brief • Ensure all activities required that are detailed in the project assignment brief are completed according to the agreed schedule • Agree a plan for producing an early engagement report • Participate in post project reviews • Produce the post implementation report and gain agreement from Service Providers and the Department • Ensure the project have allocated resources accordingly to manage and create an architectural design for each of the environments/components specified in the environment design and delivery strategy • Produce the environment design and delivery strategy • Produce, deliver and obtain sign-off of the architectural design • Review Service Providers proposals and collate a costed proposal for each environment/component specified in the environment design and delivery strategy	• Support SIAM in understanding the project requirements and assist in the production of the project assignment brief response • Execute all activities required that are detailed in the project assignment brief response • Review requirements and contribute to the environment design and delivery strategy • Review and agree the architectural design • Produce costed proposals for the Service Providers elements of the architectural design • Support SIAM in the review of the environment sign-off criteria and provide comments to the Department

6.2 Project Management

……Continued

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
	• Throughout the process, provide status reporting to the Department on progress against delivery plans • Ensure alignment of service management designs to the Department's service models and standards	• Provide detailed delivery plans for each of the environment/components specified in the environment design and delivery strategy and deliver according to the plan • Perform all Service Providers activities identified in the baselined plan and participate in the decision of whether the project should go live • Provide input to the post implementation report
Key metrics	**Key metrics**	**Key metrics**
	•Baselined Project delivery plans established within x weeks of initial engagement for x% of Projects. •No more than x% of Projects implemented with non-standard technology •Reduce the average time taken by Projects between Technical Review and Operational Readiness Review by x% year on year •At least x% of project milestone deliveries are met in accordance with agreed delivery plans	

6.3 Release & Deployment

Description	Outcomes
Ensures releases are deployed in to the Production Environment in order to deliver value to client Department and be able to hand over service to operations	• Ensure that Projects deliver services designed for successful operational delivery of business requirements; • Ensure that Projects deliver operable solutions • Provides assurance that the hardware and software in use within the Department is of good (or known) quality because releases are built properly and have been subject to quality control and effective testing • Reduces errors through the controlled release of hardware and software to the Department's live environment • Minimises the disruption of the service to the business through synchronisation of releases within packages

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Not Applicable	• Develop, maintain and communicate the Release Management strategy • Review and consolidate the Service Providers draft implementation plans • Consolidate build documentation • Manage the draft consolidated implementation schedule and plan and provide progress updates to the Department against the schedule and plan • Manage the implementation, confirm Service Providers and the Department readiness to proceed with the project go-live • Ensure releases are packaged in accordance with the Release Management strategy • Verify deployment has been successfully completed to all relevant stakeholders	• Provide Service Providers draft implementation plans to SIAM • Perform allocated Service Providers activities on the draft consolidated implementation plans • Attend and contribute to the implementation walkthrough • Provide Service Providers product catalogue, release plans and roadmaps to SIAM • Package releases in accordance with the Release Management strategy • Provide early life support immediately after deployment
Key metrics	**Key metrics**	**Key metrics**
	•Less than x% of releases managed through Service Transition Planning and Support to be reverted to previous version •x% of package releases are standard	

6.3 Release & Deployment

Description	Outcomes
Ensures releases are deployed in to the Production Environment in order to deliver value to client Department and be able to hand over service to operations	• Ensure that Projects deliver services designed for successful operational delivery of business requirements; • Ensure that Projects deliver operable solutions • Provides assurance that the hardware and software in use within the Department is of good (or known) quality because releases are built properly and have been subject to quality control and effective testing • Reduces errors through the controlled release of hardware and software to the Department's live environment • Minimises the disruption of the service to the business through synchronisation of releases within packages

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Not Applicable	• Develop, maintain and communicate the Release Management strategy • Review and consolidate the Service Providers draft implementation plans • Consolidate build documentation • Manage the draft consolidated implementation schedule and plan and provide progress updates to the Department against the schedule and plan • Manage the implementation, confirm Service Providers and the Department readiness to proceed with the project go-live • Ensure releases are packaged in accordance with the Release Management strategy • Verify deployment has been successfully completed to all relevant stakeholders	• Provide Service Providers draft implementation plans to SIAM • Perform allocated Service Providers activities on the draft consolidated implementation plans • Attend and contribute to the implementation walkthrough • Provide Service Providers product catalogue, release plans and roadmaps to SIAM • Package releases in accordance with the Release Management strategy • Provide early life support immediately after deployment
Key metrics	**Key metrics**	**Key metrics**
	•Less than x% of releases managed through Service Transition Planning and Support to be reverted to previous version •x% of package releases are standard	

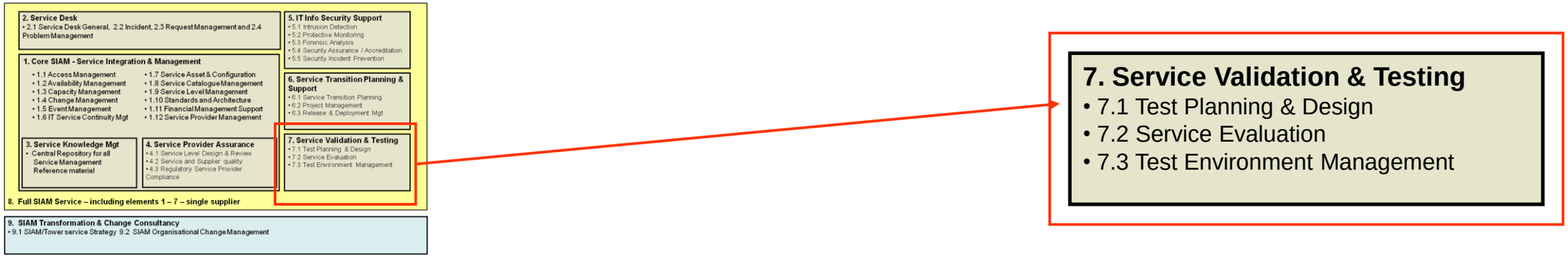
6.4 Transformation Delivery & Cost Optimisation

Description	Outcomes
Ensures transformation delivery cost reduction & ongoing cost optimisation are continually driven through	• Ensure that the cost reductions & savings from transformation are driven through to the bottom line • Ensure that services are continually driven to optimise cost throughout service lifecycle • Provides assurance that the cost optimisation is being delivered • Challenges cost of E2E services from request, through to delivery & at any point of change • Continually looks to new processes, systems or technology that can optimise cost of service delivery

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Ensures transformation delivers cost optimisation • Ensures that new services are requested based on most optimal cost basis for each requirement	• Develop, maintain and communicate the transformation delivery & cost optimisation milestone plan • Monitor & review progress against plan & report cost savings/optimisation • Continue to drive cost optimisation through new service requests or changes • Challenge service delivery costs: process, system or technology savings opportunities • Drive the cost optimisation, cost saving ethos throughout service lifecycle	• Provide Service Providers transformation delivery & cost optimisation plans • Drive transformation of service provision to delivery cost optimisation & cost saving • Proactively contribute to cost optimisation & cost saving opportunities at every stage of service lifecycle
Key metrics	**Key metrics**	**Key metrics**
	• Cost saving/optimisation x% through transformation milestone delivery plan & year on year cost reduction	• x% Cost saving/optimisation delivery - by transformation plan milestone delivery & year on year reduction

7. Service Validation & Testing



7. Service Validation & Testing
- 7.1 Test Planning & Design
- 7.2 Service Evaluation
- 7.3 Test Environment Management

Description

Service Validation and Testing provides confidence and assurance to the Department that a Project release will deliver the expected outcomes & value for the department by ensuring that the service is ‘fit for purpose’.
Service Validation and Testing consists of the following functions:-

- 7.1 Test Planning, Design and Integration – ensures that new service testing is planned and the service is designed to meet the Departments and integrated technology needs and ensures all the Service Providers components are fully and optimally integrated to provide department with stable, maintainable end-to-end service

- 7.2 Service Evaluation - evaluates the intended effects of a service change as much as reasonable practical, providing information about whether a change should be approved or not

- 7.3 Test Environment Management – ensures that the test environment is kept up to date with operational service change, ensuring testing replicates live environment

7.1 Test, Planning, Design & Integration

Description

Ensures that new service testing is planned and the service is designed to meet the Departments and integrated technology needs and ensures all the Service Providers components are fully and optimally integrated to provide department with stable, maintainable end-to-end service

Outcomes

- Manage and ensure integration of the testing of IT Projects including Operations Acceptance Test (OAT) and Service Management Acceptance Test (SMAT)
- Manage the planning, design, delivery and support of operational environments used by IT Projects for testing

Relationship & Interfaces

Customer/Service Consumer

Provide project documentation and entry criteria to SIAM and Service Provider to enable them to plan Operational Acceptance Testing (OAT) and Service Management Acceptance Testing (SMAT) phases including the Project Test Strategy

Review and agree the consolidated OAT and SMAT strategies and plans

Review and comment on progress reports provided by SIAM

Review and sign-off the OAT and SMAT test completion reports

Perform Field Acceptance Testing (FAT) and provide FAT sign-off

SIAM (Outsourced or Retained)

- Review the Department project documentation appropriate to OAT and SMAT and provide consolidated Service Provider and Service Integrators comments to the Department
- Review, optimise and consolidate Service Provider OAT and SMAT strategies and plans
- Validate and verify the test plans and designs for completeness, including all potential interfaces
- Manage the OAT and SMAT test schedule and plan and provide progress updates to the Department against the plan
- Produce consolidated OAT and SMAT test completion reports
- Manage the design and completion all end-to-end integration testing
- Provide a consolidated and integrated test report for all testing activities

Service Provider

- Review the Department project documentation appropriate to OAT and SMAT and provide comments to SIAM
- Provide OAT and SMAT strategies and plans to SIAM for review
- Perform allocated Service Provider activities on the consolidated OAT and SMAT plans
- Provide Service Provider OAT and SMAT test completion reports to SIAM and review and sign-off the consolidated OAT and SMAT test completion reports
- Review transition requirements and contribute to the transition approach
- Provide a completed Service Provider project transition plan
- Provide assurance about Service Provider deliverables and transition activity to SIAM prior to the operational readiness review

Key metrics

Key metrics

•x% of integrated test plans completed by their due date

Key metrics

7.2 Service Evaluation

Description	Outcomes
Evaluates the intended effects of a service change as much as reasonable practical, providing information about whether a change should be approved or not	• Evaluate the impact and anticipated benefits of proposed project changes including performance • Provides assurance and recommendations to the Department on the quality of changes and whether they are “fit for purpose”

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Consider recommendations from SIAM prior to approval of the Project changes	• Plan the evaluation of the Project change • Perform risk assessments based on the Department’s specifications • Develop the performance model in order to undertake effective evaluation • Provide an assessment to the Department of predicted end-to-end performance, risks and acceptability of such risks • Report on end-to-end performance following the change and provide an assessment to the Department of the actual performance against predicted performance	• Provide all relevant information required by SIAM to enable its evaluation of Project changes
Key metrics	**Key metrics**	**Key metrics**
	•x% of assessment reports produced on time •x% of assessment reports predicted end-to-end performance within x% of actual performance	

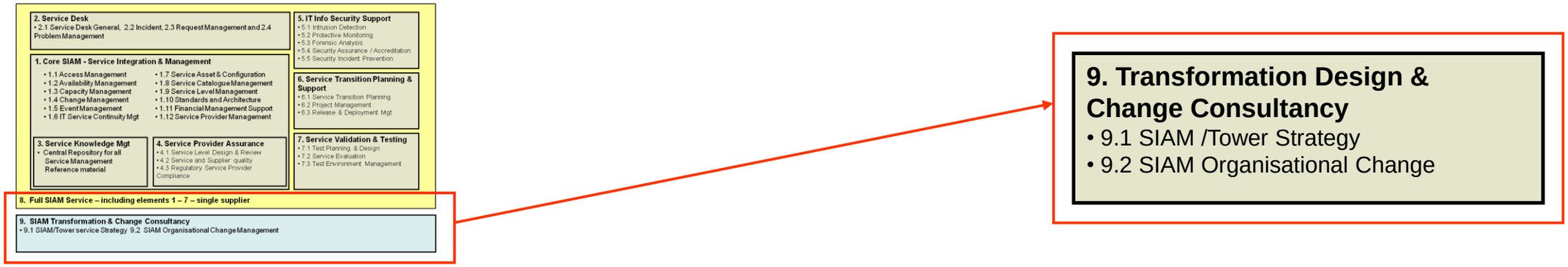
7.3 Test Environment Strategy

Description	Outcomes
Ensures that the test environment is kept up to date with operational service change, ensuring testing replicates live environment	• Demonstrate reductions in costs to the Department through increased re-use of environments year-on-year • Test environments mirror production environments thereby reducing and minimising the number of incidents post go-live

Relationship & Interfaces

Customer/Service Consumer	SIAM (Outsourced or Retained)	Service Provider
• Clean test environments when used • Maintain Service Provider test environments in line with production environments	• Ensure test environments are cleaned when used • Maintain and manage an environment resource allocation service • Update the environment resource allocation service if the environment if rolled forward from a previous release • Ensure that the proposed environment is aligned to the Department Technology roadmap and Service Provider technology roadmap • Inform the Department of any upcoming environment expiry dates at least 30 days before due expiry	• Provide information to SIAM on future Project activity to enable SIAM to assess and determine future environment availability
Key metrics	**Key metrics**	**Key metrics**
	• At least x% of test environments re-used year on year	

9. SIAM Transformation Design & Change Consultancy



Description

SIAM Transformation Design & Change Consultancy provides consultancy to support departments to design and implement their SIAM / tower service structure and consists of the following two aspects of transformational design:-

- 9.1 SIAM/Tower Strategy – supports departments in designing, planning and implementing the transformation change required to enable them to adopt and apply the SIAM / Tower model to optimise their IT service delivery. Strategy consultancy supports the Transformation to provide a SIAM/tower model that is designed to meet the Departments business and integrated IT service requirements and ensures all the components from Enterprise Architecture, retained organisation, SIAM to IT service delivery are fully analysed, designed, interfaces and boundaries are clear, through to implementation planning & programme / project managed delivery where required, to provide departments with stable, maintainable end-to-end business service

- 9.2 SIAM Organisational Change – provides cultural change consultancy & support to ensure that the people aspects of change are analysed, designed, planned and implemented to ensure successful SIAM / tower transformation

9.1 SIAM / Tower Strategy

Description	Outcomes
Ensures that transformation is designed, planned and implemented to meet the departments business requirements maximising value for money with minimum business/operational disruption	• To ensure optimal transformation from current to future state IT service provision • Moving to E2E business service, consumption based, agile, commoditised IT services using a multi-source, value for money mix of service providers

Relationship & Interfaces

Consultancy	Retained Organisation	SIAM/Tower Service Provider
• Provide SIAM/tower technical expertise to support department to design SIAM/tower model strategy • Provide business analysis to understand current state • Provide SIAM/tower technical expertise to support enterprise architecture and retained organisation design optimal SIAM/tower future state • Provide planning expertise to support creating high level and detailed plans to take the department from current state to future state • Provide programme and project management expertise and support to implement the SIAM/tower model and successfully complete the SIAM / tower transformation to business as usual – stead state, realising benefits of the transformation	• Provide details of current IT service operation, access to service owners and service documentation • Provide input and business requirements to SIAM / tower strategic vision • Validate and verify current state analysis • Review, test and sign off future state design • Provide governance and resource as required to achieve transformation • Review and sign off each transformation delivery milestone • Act as primary interface with any potential SIAM/tower service provider • Retain responsibility for all procurement activity (specifically excluded from consultancy)	• Work with the Consultancy provider to deliver the transformation required by the Retained Organisation
Key metrics	**Key metrics**	**Key metrics**

9.2 Organisation Change

Description

Ensures that the people and cultural aspects of SIAM/tower transformation are supported to facilitate rapid change implementation and embedding

Outcomes

- Ensure that the people and cultural change is designed, planned and implemented to support and facilitate successful transformation being completed and embedded within the retained organisation supporting the technical/service provider transformation

Relationship & Interfaces

Consultancy

- Provide Organisational, People & Cultural change expertise to support department to design SIAM/tower model strategy
- Provide organisation structure expertise relating to SIAM/tower transformation design
- Provide planning expertise to support creating high level and detailed plans to take the department from current state to future state in relation to organisation cultural change
- Provide technical expertise to support retained organisation engagement, communication, job re-engineering, training, implementation and embedding delivery

Retained Organisation

- Provide details of current IT service organisation, access to service team leads and service job roles
- Provide input and business requirements to SIAM / tower strategic people vision: capability, skills, training
- Validate and verify current state analysis: retained organisation
- Review, test and sign off future state design: retained organisation
- Provide governance and resource as required to achieve transformation for retained organisation
- Review and sign off each transformation delivery milestone for retained organisation
- Act as primary interface with any potential SIAM/tower service provider
- Retain responsibility for all procurement activity (specifically excluded from consultancy)

SIAM/Tower Service Provider

- Work with the Consultancy provider to deliver the transformation required by the Retained Organisation

Key metrics

Key metrics

Key metrics