ITIL®

An example ITIL® -based model for effective Service Integration and Management

Kevin Holland

AXELOS.com

AXELOS GLOBAL BEST PRACTICE

White Paper
April 2015

Contents

Foreword

ITIL® has always, quite rightly, promoted the primary importance of managing the end-to-end service that IT delivers to their customers. The increasing complexity of the IT value chain and the rise of multi-vendor supplier eco-systems has led to the rise of Service Integration and Management (SIAM) as a new approach.

SIAM is a relatively new, and fast evolving concept, but it is far from being theoretical. SIAM providers are being established as part of some of the largest strategic sourcing initiatives around the world and across many different sectors.

In his first White Paper on SIAM, 'An introduction to Service Integration and Management and ITIL', Kevin Holland cogently argues that a successful implementation of SIAM rests upon the guidance provided by ITIL whilst also highlighting the need to adopt and adapt the guidance it contains to reflect the multi-tenant model. He also provides an overview of the drivers for developing a SIAM strategy and the specific challenges that it generates.

As Kevin states in that White Paper the IT industry has yet to develop an authoritative model for describing SIAM, and the objective evidence does not yet exist to reliably assess whether any specific option for SIAM is more or less effective.

In this second White Paper Kevin describes one example model for effective SIAM. This model is based on an implementation already in use within the UK public sector.

The two White Papers are a major step forward in the global, industry wide dialogue that needs to precede the development of an authoritative set of SIAM guidance.

James Finister, Tata Consultancy Services

1 Introduction to Service Integration and Management

The first White Paper on SIAM, 'An introduction to Service Integration and Management and ITIL', provided a detailed introduction to the topic, and should be read before this White Paper. Some of the key aspects are reproduced in this White Paper to assist the flow and to aid understanding.

The purpose of this White Paper is to provide one example model for effective Service Integration and Management (SIAM), including example functions and techniques. This model is founded on one that has proven its value in managing a complex multi-supplier environment since 2003. The benefits described in the first White Paper have been achieved through the application of this example model, and are reproduced in chapter 9 of this White Paper. Other models are also in use.

This paper is intended for:

- IT Service Management (ITSM) professionals already using ITIL in a multi-supplier environment
- ITSM professionals who understand ITIL and its benefits, and want to adopt ITIL for their multi-supplier management requirements
- IT service providers (internal and external to an organization)
- SIAM providers
- SIAM consultants
- ITSM practitioners and consultants.

1.1 WHAT IS SERVICE INTEGRATION AND MANAGEMENT?

Service Integration and Management (the abbreviation SIAM will be used from this point for brevity) is an adaptation of ITIL that focuses on managing the delivery of services provided by multiple suppliers.

SIAM is not a process. SIAM is a service capability and set of practices in a model and approach that build on, elaborate, and complement every part of the ITIL practices.

The aim of SIAM is to provide a single point of visibility and control for the service management and delivery of all services provided by suppliers, by:

- Taking end-to-end accountability for the performance and delivery of IT services to the users, irrespective of the number and nature of suppliers
- Coordinating delivery, integration, and interoperability across multiple services and suppliers
- Assuring suppliers performance
- Ensuring that the services effectively and efficiently meet the business need
- Providing the necessary governance over suppliers on behalf of the business.

Adopting a SIAM model will require changes to ways of working in the business, the suppliers, and the SIAM provider. This White Paper provides examples of the nature of some of the changes that may be required, but is not exhaustive.

2 An example SIAM model

2.1 HIGH LEVEL CONCEPTUAL MODEL

Figure 2.1 provides a high level conceptual illustration of SIAM. This shows the SIAM provider in the centre, acting as the bridge between the users (service consumers) and the suppliers of the services. The SIAM provider provides a SIAM capability as a set of services.

A homogeneous SIAM model provides consistency for the governance, management, and coordination for all services, irrespective of the type of services, organizational relationships with the suppliers, type of supplier, type of service consumers, or number of different parties.

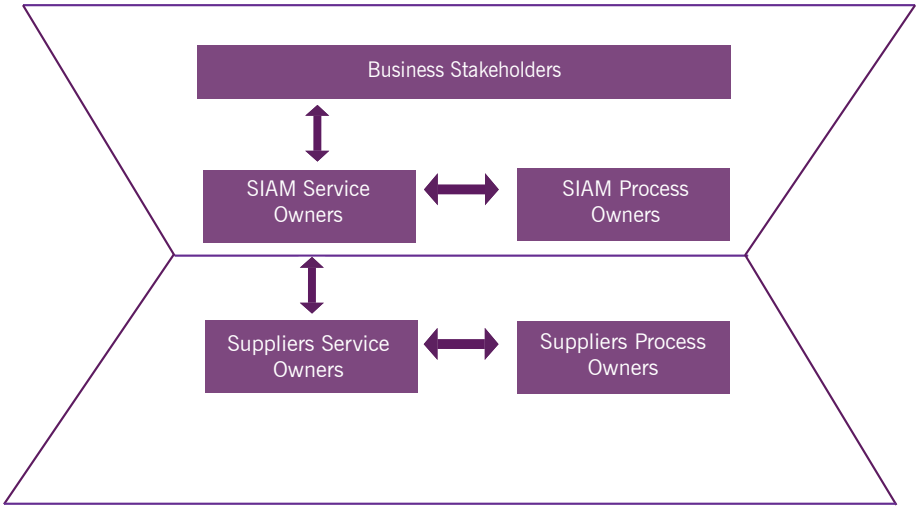

Figure 2.1 High-level conceptual illustration

The SIAM provider may be provided from within the business, outsourced to one of more SIAM providers, or a combination. The SIAM component model helps to determine the most appropriate approach.

2.2 SIAM COMPONENT MODEL

SIAM is not one thing. SIAM is a set of capabilities each of which has its own processes, functions, activities, and principles. A SIAM model logically groups these capabilities into related components. This grouping aids the understanding of what SIAM is, supports informed sourcing decisions, and ensures that focus is given to the activities essential for effective SIAM.

A SIAM provider cannot operate in isolation. As well as the suppliers of the IT services, a SIAM provider also needs specific support from the business organization in areas that typically include:

- **Enterprise architecture:** The process of translating business vision and strategy into effective enterprise change by creating, communicating, and improving the key principles and models that describe the enterprise's future state and enable its evolution[1]
- **Programme management:** Managing a set of related projects that delivers a strategic goal in order to realize specific benefits, including managing realization of those benefits
- **Project management:** Planning and organizing individual business projects to achieve specific goals
- **Systems integration:** Getting solutions, differing technologies, applications, and infrastructure to work together, with a focus on technology integration
- **Commercial procurement:** The coordination and management of buying goods and services, including the formulation, negotiation, and agreement of legal contracts
- **Business analysis:** The capture and analysis of business requirements for new and changed services.

External organizations can provide assistance to the business for these support areas, but the overall accountability and control must remain within the business.

Figure 2.2 illustrates one example of a SIAM model that has been broken down into components. This is based on the UK Public Sector's SIAM Enterprise Model, which was first created in 2012. This model and variations of it have been widely adopted in UK public sector organizations. The example model can be used when designing or reviewing specific SIAM models to initiate detailed review and discussion, and to ensure that all of the aspects included are considered.

Other SIAM models are in use, but many of them share a similar set of components.

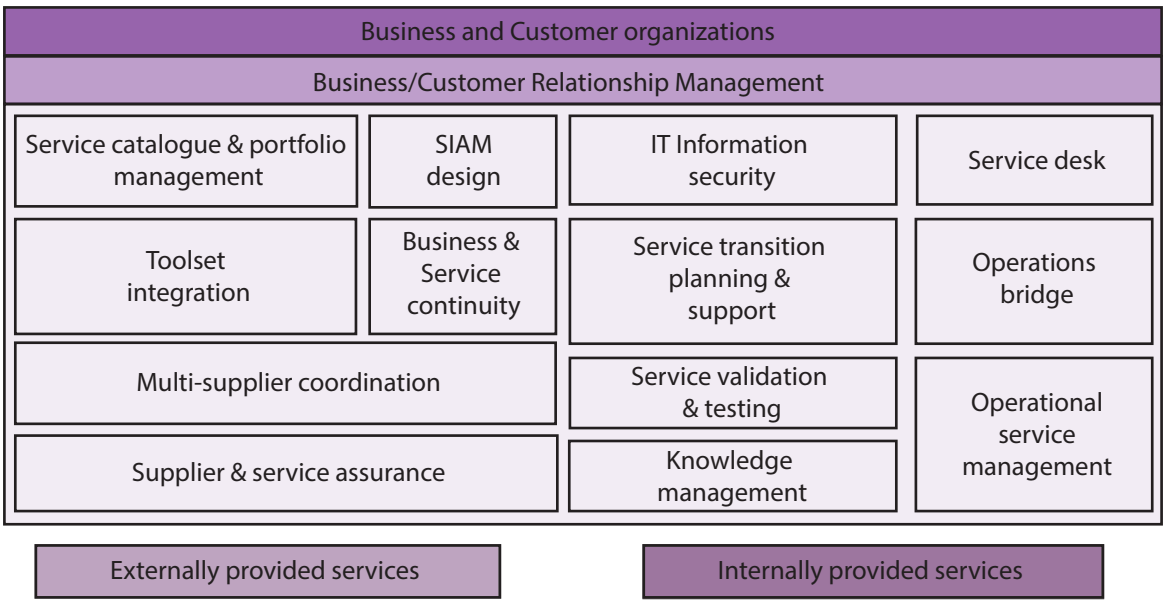

Figure 2.2 SIAM component model

'Core' SIAM components have the title highlighted. See chapter 3.1 for further information.

Integrating services is in itself a service, and each component of this SIAM model can be delivered as a service.

The delivery of each component may be sourced from within the business or externally sourced, or in combination. External sourcing can be to a single or multiple specialist providers of SIAM services. The sourcing choice depends on:

- The existence of SIAM capability in the business
- The maturity of that SIAM capability
- The capacity of the SIAM capability
- The size and complexity of the business
- The size and complexity of the services
- The size and complexity of the supplier landscape.

It is becoming increasingly common to have one principle provider for the SIAM components, but also use other specialist providers for some of the components, either to:

- Use best of breed, specialist providers for specific components (for example, performing security penetration tests)
- Increase capacity (for example, using a specialist provider of testing services to meet a peak in demand)
- Address gaps in capability and maturity for specific components (for example, knowledge management specialist providers).

Where this is the case, the principle SIAM provider will have the responsibility for integrating the other SIAM providers, and will retain overall accountability.

3 SIAM component descriptions

The SIAM Enterprise Model includes a number of individual SIAM components, each of which focuses on specific related processes and activities. A summary of these is provided below. Chapter 4 includes some key examples of use and adaptation of ITIL processes and techniques.

The model is not intended to be an organizational model, although some of the components are often aligned to specific organizational units where these require specific focused skills. Typical examples of aligned components are:

- IT information security
- Service validation and testing
- Service desk
- Operations bridge.

To illustrate this, it is perfectly feasible and acceptable for a single person to execute activities that span several SIAM components. For example, a specialist in IT service continuity (ITSC) could be involved in providing the capability for all of the following SIAM components:

- **Supplier and service assurance**: conducting a maturity assessment of a suppliers ITSC capability
- **Service validation and testing**: reviewing the test results from a suppliers disaster recovery test
- **Business and service continuity:** Creating the top level plan that integrates all of the suppliers ITSC plans, determines the overall risks to the customer organization, and establishes mitigation
- **SIAM design:** designing the service configuration to mitigate against risks, for example by specifying the use of two different providers of Infrastructure as a Service with live instances of critical applications shared across them.

The components must be fully integrated. For example, although IT information security includes security incident and event management, this must be fully interfaced to the incident management process of the Service Desk, and the event management process of the Operations Bridge so that security incidents and events can be managed through the lifecycle, irrespective of how they are initially detected and reported.

3.1 CORE SIAM

The first sets of components are grouped into what is often referred to as ‘Core SIAM’, as these are common to every SIAM model and form the heart of what a SIAM provider should do.

3.1.1 SIAM Design

This component is concerned with the creation, updating, and improvement of the specific SIAM operating model. This includes the design of necessary processes policies and templates, information exchanges necessary for integration, SIAM organizational structures, impact assessment of new services against the model, design of appropriate metrics, and the design of service level models.

There must be a single documented design for SIAM. Where the SIAM capability is provided externally to the business, the business should have rights to use the design in order to avoid lock-in to the particular SIAM provider. This design must be subject to change management, with any changes being impacted by the SIAM provider, the business, and the suppliers.

The processes are:

- Design coordination
- Availability management design
- Capacity management design.

3.1.2 Service Catalogue and Portfolio Management

This component is concerned with the creation and management of the Service catalogue and portfolio management that are used by the SIAM provider, the suppliers, and the business to support delivery of the services.

The principles, methods and techniques for design and creation of these catalogues are not elaborated here as they are fully described in the ITIL Service Strategy and Service Design publications.

The processes are:

- Service portfolio management
- Service catalogue management.

3.1.3 Toolset integration

This component is concerned with the integration of the toolsets used by the SIAM provider and the suppliers. This includes the selection, implementation, and configuration of appropriate SIAM tools to support the SIAM model. SIAM tooling includes:

- Tools to support the execution of processes within the SIAM provider
- Service alerting and monitoring tools
- Decision support systems
- Diagnostic tools
- Discovery tools
- Security tools
- Reporting tools
- Analytical tools.

The component is also responsible for integrating the supplier's toolsets with all of the above. The tooling strategy must consider the impact on replacing any of the suppliers of the services or the SIAM components.

Most suppliers will already have their own tools, used to serve multiple customers and often also multiple service integrators. This presents challenges to integrating these toolsets with other suppliers and with the SIAM provider. See the first White Paper, 'An introduction to Service Integration and Management and ITIL', for information on strategies for tooling.

3.1.4 Multi-supplier coordination

This component is concerned with the activities necessary to coordinate the process execution across multiple suppliers to ensure seamless operation of the services to the users. This includes providing the capability to highlight the potential impact of the activities of one supplier on the services of another supplier, so that any adverse impacts can be predicted and prevented. The processes include:

- Change management for changes that affect multiple suppliers (see ICAB in chapter 6)
- Release planning and release conflict resolution (see R&MP, chapter 6.4)
- Capacity management providing the demand to all affected suppliers
- Major incident management for major incidents involving multiple suppliers (see Service Bridge, chapter 6.5)
- Problem management for problems involving multiple suppliers
- Innovation
- Continual service improvement.

3.1.5 Business and service continuity

This component is concerned with the activities necessary to create and maintain the integrated business and service continuity plans, including design, implementation and improvement of processes,

creation, maintenance and testing of the integrated continuity plans, testing, and maintenance. The processes are:

- IT service continuity management
- Business continuity management.

3.2 REMAINING SIAM COMPONENTS

The other SIAM components are:

- Business/customer relationship management
- Financial management
- Knowledge management
- Supplier and service assurance
- IT Information Security
- Service transition planning and support
- Service validation and testing.

3.2.1 Business/customer relationship management

This component is concerned with building and maintaining the relationships between the SIAM provider, the business, and the customers of the services. The concept of Service Owners is used to support this (see chapter 4.2).

Having positive and productive relationships with the business and the customers is crucial to effective SIAM. The SIAM provider acts as the agent of the business, and must be seen to be part of it and represent its views. Ideally the SIAM provider will have representation on the management board of the business.

Some businesses choose to retain customer relationship management. This is perfectly acceptable, however the precise responsibilities for specific activities must still be defined (see chapter 4).

The processes are:

- Business relationship management.

3.2.2 Financial management

This component is concerned with financial management of the SIAM provider, the suppliers, and the services, including understanding and monitoring the costs against budgets, accounting, and charging.

Typically the business will establish and own the budget, ideally with support from the SIAM provider. The SIAM provider then has responsibility for working within the budgets to deliver the service.

One critical aspect is establishing a robust cost model so that the cost of each service, including the SIAM overhead for the service, are known, measured, and monitored. The SIAM provider must be able to justify the costs of its service against its responsibilities and the quality of service delivered.

The processes are:

- Financial management.

3.2.3 Knowledge management

This component is concerned with the creation, maintenance, analysis, publication, and sharing of all knowledge necessary for effective operation of the SIAM model. It also includes managing shared information repositories that can be accessed by all suppliers, customers, and the SIAM provider using appropriate access controls. The knowledge is sourced from, and should be shared between, all suppliers and the SIAM provider, and should include:

- Documentation describing the processes, policies, and templates
- User manuals
- Known errors from every supplier and service

- Descriptions and illustrative diagrams of the services
- Service interfaces, both within a supplier and between suppliers
- Operational data
- Reports on achievement of service levels, for individual services and for the end-to-end services
- Key performance indicators for the services, the suppliers, and the SIAM provider.

The processes are:

- Knowledge management
- Service asset and configuration management.

3.2.4 Supplier and service assurance

This component is concerned with the assurance of the suppliers, services, and the SIAM provider itself, managing the performance of the suppliers and the services against service levels and ensuring adherence to agreed requirements. This includes carrying out:

- Service level management
- Audits to ensure that processes are being followed
- Assessments of process maturity and capability
- Assessments of suppliers maturity and capability
- Test assurance of suppliers testing
- Audits of compliance against requirements
- Audits of compliance against standards
- Monitoring of CSI initiatives to ensure that they are being actioned.

The processes are:

- Service review
- Service level management
- Process evaluation
- Monitoring of CSI initiatives.

If the SIAM provision is outsourced, then the business must still retain the capability for this component in-house in order to effectively manage the SIAM provider. This is required to provide the business with the confidence that the SIAM provider is meeting its obligations.

As the skills for performing supplier and service assurance over individual suppliers are largely the same, businesses should seriously consider retaining the capability for this component in-house for managing all suppliers of the IT services. This approach is becoming increasingly common.

3.2.5 IT Information Security

This component is concerned with all aspects of information security management for both the SIAM provider and the suppliers. This includes:

- Security design
- Security testing
- Security risk assessments
- Security incident monitoring and management
- Security event monitoring and management
- Audit logging
- Protective security monitoring
- Forensic analysis
- Security assurance
- Accreditation of suppliers and services.

The focus should be on creating one security community that includes the SIAM provider and all suppliers and customers. For example, if one supplier discovers a vulnerability in a particular component, they should inform the SIAM provider. The SIAM provider should then make all other suppliers aware, so that they can check if they have the same vulnerability. The SIAM provider would then manage addressing the vulnerability across all suppliers, acting as if they were all part of the same organization.

The processes are:

- Information security management.

3.2.6 Service transition planning and support

This component is concerned with the integrated planning and management of the transition into live operation of new and changed services that involve multiple suppliers, the retirement or transfer of services, and the transition and introduction of new services and new suppliers into the SIAM model (see Service Introduction, chapter 6.7). Suppliers retain responsibility for the release and deployment management of their own services. This component includes:

- Planning of the integrated releases and deployments
- Release and deployment management of the integrated releases
- On-boarding of new suppliers and services
- Service acceptance, including operation of defined gateways
- Service retirement
- Transfer of services from one supplier to another.

On-boarding and off-boarding of suppliers needs particular focus.

The processes are:

- Release and deployment management
- Change evaluation
- Project management (transition planning and support).

3.2.7 Service validation and testing

Suppliers should be fully responsible for the testing of their own services. This component is concerned with the assurance of suppliers testing, with the SIAM provider performing a review and quality assurance role. It is also concerned with the integration testing of new and changed services that involve multiple suppliers, any system integrators, and project teams to ensure that the services will work correctly together.

Both supplier testing and integration testing should cover both utility and warranty aspects, including the testing of component and end-to-end performance and resilience. Suppliers can also conduct their own integration testing with other suppliers, and should be encouraged to do so. However, the SIAM provider should retain the overall accountability and assurance. This component includes:

- Design of integrated tests
- Test planning and coordination
- Integration test execution
- Ownership and maintenance of common regression tests
- Management of integration test environments
- Management of test data for the integration tests.

The processes are:

- Change evaluation
- Service validation and testing.

3.3 OPERATIONAL MANAGEMENT SIAM COMPONENTS

The following components focus on operational management rather than governance. It is useful to include them in the SIAM model as this supports standardization and economies of scale. These capabilities can be provided to both internal and external suppliers.

3.3.1 Service desk

This component provides a service desk function for the SIAM model. This is often the sole service desk for all services. In some SIAM models users report all incidents to the SIAM service desk, who then escalate unresolved incidents to the appropriate supplier. This model provides users with a single point of contact, but may not always be the best model as it adds an additional handoff point between the user and the suppliers.

An alternative model allows users to report incidents directly to the service desk of the supplier. This removes one step from the end-to-end incident resolution process, but can only work where it is clear to the user who is the supplier of the service. This can be achieved if the service lines are aligned to the services directly consumed by the user.

The incident management and event management processes must be fully integrated with the other SIAM components, in particular the Operations Bridge and IT Information Security.

The processes are:

- Incident management
- Request fulfilment
- Access management.

3.3.2 Operational service management

This component provides a service management capability for the processes from Service Operation and Service Transition, including those listed below, as a ‘shared service’. Any suppliers can elect to engage a SIAM capability to perform activities such as change management and problem management, but this is typically only advantageous to internal suppliers or very small external suppliers. Whilst the other SIAM components provide the necessary governance, coordination and integration capabilities, this component provides the operational capabilities. These are fully described in ITIL.

The SIAM provider must be careful not to allow a ‘flow up’ of operational service management activities into the SIAM provider from the supplier, unless this can be proven to add value and improve the service. This is particularly the case where the supplier provides a ‘managed service’, with full responsibility for delivering the service to service levels. If the SIAM provider carries out specific service management tasks, they are then taking over responsibility from the supplier, and hence now own the associated risks of poor delivery. A good example of where this has unfortunately happened in some SIAM implementations is configuration management, with the SIAM provider trying to maintain a CMS that contains all assets used by all suppliers (see chapter 6.9).

The processes are:

- Incident management
- Problem management
- Change management
- Release and deployment management
- Service validation and testing
- Service asset and configuration management
- Capacity management
- Availability management
- IT service continuity management.

3.3.3 Operations bridge

This component provides a single IT operations function, carrying out activities including service monitoring and alerting, event management, housekeeping, healthchecks, and batch management as a 'shared service'. Any suppliers can elect to engage this SIAM capability to perform these activities, but this is typically only advantageous to internal suppliers or very small external suppliers.

The processes are:

- IT operations control
- Technical management
- Event management
- Incident management.

4 How to use this component model

This component model has been successfully used when designing specific operating models for SIAM. It should be considered as the basis for detailed iterative review and discussion in order to establish the most appropriate operating model for a particular business:

- Services
  - What are the required business services?
  - Who are the consumers of the business services?
  - What are the supporting services that are to be provided by the suppliers?
  - What are their boundaries and interfaces between services?
  - What are the necessary interactions between each service?
  - Which services could be provided internally?
  - Is there any logical grouping of services that could be provided by the same supplier as a service line?
- Supporting functions
  - Can the business provide all of the necessary supporting functions?
  - If not, how could they be sourced?
- SIAM components
  - Does the proposed SIAM operating model cover all of the necessary SIAM components?
  - What are the required characteristics for each SIAM component, e.g. hours of service
  - For the specific business environment, are any additional SIAM components required?
  - What capability and capacity already exists in the business for providing each SIAM component?
  - Are there specialist providers for specific SIAM components that could provide cost effective services of the necessary quality?
  - For each SIAM component, what is the best sourcing strategy? This helps to avoid an uninformed decision to 'outsource all' when the business already has some or all of the capability.
  - If a single outsourced SIAM provider is being considered, do they provide best value for all of the components?

Once these and an appropriate sourcing strategy have been determined, the model and the components should then be used to define and document the roles and responsibilities of:

- The business organization outside SIAM
- The customers
- The provider(s) of the SIAM components
- The suppliers of the individual services and service lines under SIAM
- Any suppliers of services not under SIAM (including any IT function in the business)
- The suppliers of any outsourced business processes.

Understanding and agreeing roles and responsibilities at the outset is critical to the success of SIAM, otherwise quality of service will suffer and costs will increase.

Swim-lanes are a useful technique for modelling the process flow and responsibilities for each process step. This visual representation helps to highlight process complexities and complex hand-offs between participants, so that they can be designed out.

Once the optimal process flows have been established, a RASCI (Responsible, Accountable, Supports, Consulted, Informed) matrix should be created. This forces consideration of accountability and responsibility, but also considers who should be consulted on each activity, who actively supports, and who is just informed. Here is an example:

Process area	Activity	Business	SIAM provider	Supplier
Capacity management	Obtain future business demand forecasts	AR	S	C
Capacity management	Collate demand forecasts	S	AR	
Capacity management	Share demand forecasts with suppliers		AR	I
Capacity management	Provision capacity to meet demand	I	A	R
Capacity management	Assure capacity plans		AR	S

Table 4.1 Example RASCI matrix

The RASCI matrix and process flows can then be used as the basis for developing any necessary contractual schedules, operating level agreements, service level agreements, and detailed service catalogues.

5 Defining service lines

Correctly designed SIAM models can integrate, manage and govern a wide variety of different services, suppliers, and sourcing approaches for the SIAM components.

In order to obtain an optimal balance between service complexity and integration complexity care must be taken to define appropriate service lines (sometimes referred to as 'Towers'). This definition should include consideration and a precise establishment of who are the consumers and recipients of each service line. Using this approach will support comprehensive understanding and effective design.

The ultimate aim should be to minimize dependencies between service lines (as this will reduce the workload and hence the costs and complexity of the SIAM provider) whilst utilizing 'best of breed' services and suppliers. Achieving this aim is highly dependent on:

- Pre-existence of services and suppliers that will continue
- Availability of suitable alternative and new services
- Types of service (e.g. bespoke, commodity)
- Costs of transition to desired service lines
- Systems integration challenges and costs
- Technical standards.

For many organizations the service lines will already be determined, as they will be the groups of services provided by existing suppliers, with either no desire to move away from them, or long term contractual arrangements.

For others who are changing suppliers at the same time as adopting a SIAM approach, this can be an opportunity to review the services that are required and group them into appropriate service lines.

The following chapters illustrate two different common approaches to service lines.

5.1 ALIGNMENT BY TECHNOLOGY

Some SIAM models align service lines along technologies, often referred to as Towers. The intent of the Tower approach is to align services with those available from pre-determined procurement frameworks, in order to support better understanding of price and performance.

Using such a construct of buying 'industry standard services at market competitive pricing' can often be a first good step to delivering significant benefit whilst a business moves from the single contract approach of the past to a multi-sourcing model.

Most Tower models have a single supplier providing the Tower service, but it is possible to have multiple suppliers in a single Tower to provide competitive tension, with the integration between them being managed by the SIAM provider. This would increase the integration complexity.

Taking this approach can provide minimum service complexity, but is likely to increase integration complexity. The services consumed by many users are likely to depend on all of the Towers, with consequent high levels of interaction between the Tower suppliers and consequent SIAM provider workload.

A typical example has the following Towers/service lines:

- Hosting
- End User Computing
- Application Management
- Network.

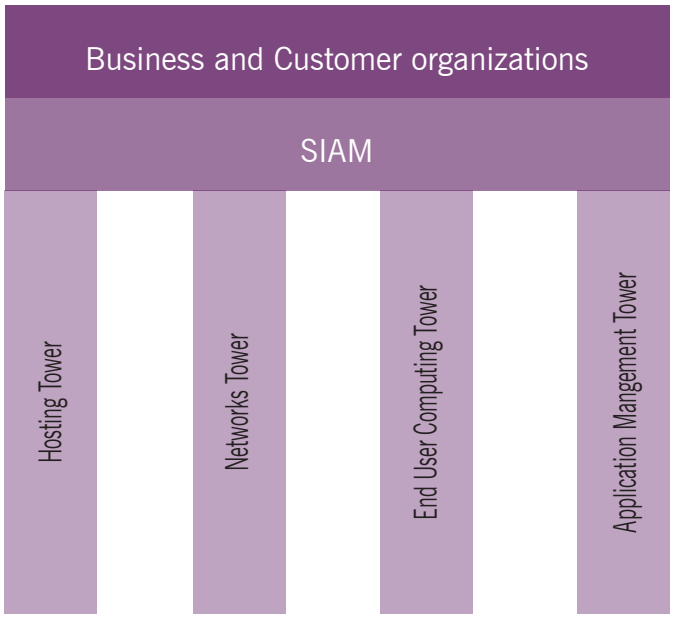

Figure 5.1 Alignment by technology

If a technology aligned model like this is adopted, the following challenges must be considered when contracting with a SIAM provider and suppliers:

- It is more likely that a Tower supplier will use a sub-contractor, where it does not have the specific capability for one aspect of the service, e.g. support for a particular niche application. This sub-contracting can lead to a loss of transparency in the supply chain, with a risk that issues with sub-contractor delivery may be hidden from the SIAM provider
- There are likely to be a high number of dependencies between services. This increases daily interactions, costs and complexities. In turn this increases the workload of the SIAM provider and of the suppliers, and crucially can affect service. For example delaying incident resolution as incidents have to be passed between suppliers
- The End User Computing and Application Management suppliers may each provide a large number of individual services. This makes it more challenging to change the supplier of one of these services, reducing the flexibility that SIAM approaches can offer.

As a further illustration of the challenges that need to be considered by using service lines of this nature, consider a business that has as one of their services a specific legacy application that has been developed to run on a bespoke hardware configuration, and with a bespoke desktop client. If the service lines above are adopted, the following challenges may need to be considered and addressed:

- The Hosting supplier may not have the knowledge and skills required for the bespoke hardware configuration. This could necessitate a re-development of the application to run on commodity hosting technologies, or costs incurred to replicate the configuration and obtain the necessary support skills. There may also be challenges in resolving issues of slow application performance, as it may not be clear if it is the Hosting or the application itself that is causing the problem
- The Application Management supplier may not have the knowledge and skills required for the legacy application. This could result in extended fix times for incidents and problems, or costs incurred to obtain the necessary support skills or to sub-contract to a specialist provider
- The End User Computing supplier may not have the knowledge and skills required for the legacy application client. This could result in extended fix times for incidents and problems, or costs incurred to obtain the necessary support skills or to sub-contract to a specialist provider. There may also be a high number of incidents passing between this supplier and the Application Management supplier, resulting in extended incident fix times.

5.2 ALIGNMENT BY SERVICE

An alternative approach is to align service lines with available services instead of technologies. This can be particularly applied to cloud services such as Software as a Service (SaaS), where splitting out hosting would create unnecessary interfaces and complexities, and to legacy services as described in the example above.

If is also usefully applied where there is a one to one relationship between the business service consumed by users and the service provided by the supplier, e.g. a Payroll service.

This alternative approach is likely to result in a greater number of suppliers, but if carefully designed can achieve minimum integration complexity and hence higher service quality and lower overall costs. The SIAM model described in this white paper can accommodate any number of suppliers and service lines. There is however an optimal balance between the number of service lines/suppliers and overall costs. As the number of suppliers and service lines increases, resource levels in the SIAM provider will need to increase due to the need for managing each supplier.

Where possible, the design of services and design of service lines should be done together using the following considerations:

- Group services into a service line only where that offers the best value and best quality of service, for example where one supplier specializes in those services
- Review system architectures in order to take advantage of pre-existing commodity services (for example Hosting, and Cloud storage)
- Match service lines to supplier offerings and capabilities (for example, different service lines for IaaS and PaaS)
- For a bespoke legacy application consider retaining a single service line for all aspects required to support it
- Create a single service line for a self-contained service provided to a specific customer or group of customers (for example, email).

A typical example could include the following service lines, each provided by different suppliers. The example has a mix of technology alignment (IaaS and PaaS), and service alignment. This mixture is often the best approach to defining appropriate service lines:

- Cloud email (includes hosting)
- Infrastructure hosting (IaaS)
- Platform hosting (PaaS)
- Application support

- Payroll application hosting and support
- Legacy application hosting and support
- Desktop support
- Network.

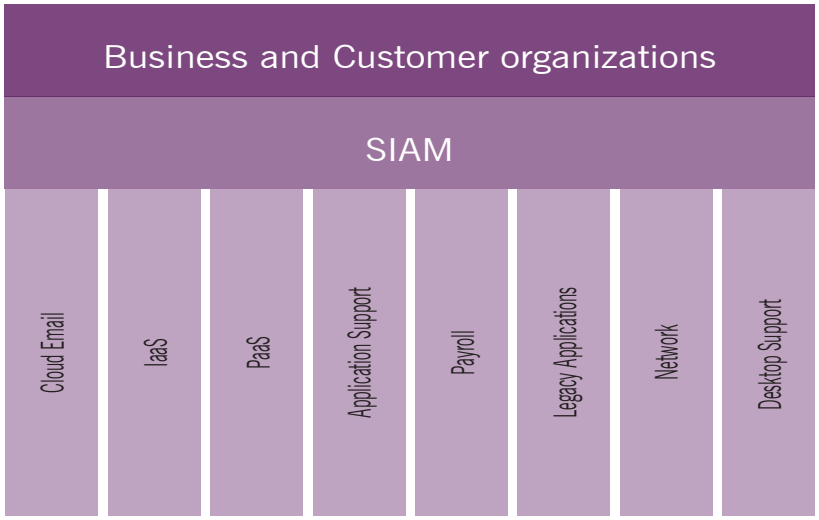

Figure 5.2 Alignment by service

This approach largely negates the challenges described for the Technology aligned service lines.

6 Adaptation of processes, functions, and techniques

Focusing on processes and technology alone will not deliver the expected benefits. Effective SIAM requires consideration of People, Process, Partners, and Products.

This includes considering data, governance, and a culture of collaboration. This chapter describes some of the adaptations of ITIL processes, functions, and techniques that are necessary for effective SIAM.

In a SIAM model, the SIAM provider is primarily concerned with providing governance over and co-ordination of the internal and external suppliers. Hence the SIAM provider's use of the ITIL processes, functions and techniques is different to those of an IT service provider.

6.1 PROCESS OWNERS

In a SIAM model, the goal is that every party should be seen to act as one. From an end user perspective, it must seem as if all services are being provided from the same organization, with the integration being invisible to the users. Process design must ensure the minimum number of hand-offs between different parties, and facilitate wherever possible process flows between suppliers without the need to go via the SIAM provider.

To enable this, and to support the necessary culture of collaboration, every ITIL process should have an identified Process Owner both in the SIAM provider and where possible in the suppliers.

The SIAM process owner has overall accountability for the design of their process across all parties, SIAM provider and suppliers, including the interfaces to related processes and between parties.

Each supplier process owner is responsible for the design of the process and interfaces within their own organization. They are also accountable for the execution and control of their process in their own organization.

It is possible for one individual to be the Process Owner for several processes. If the SIAM is retained in the business, then a SIAM Process Owner can also be the process owner for any internal suppliers.

The Process Owners within the SIAM provider are accountable for that process both within the SIAM provider and across all suppliers. This extends this ITIL role across the multi supplier environment. For each of their processes, the SIAM Process Owner is responsible for:

- Ensuring that every supplier has a Process Owner for the process
- Building an effective relationship with the suppliers process owners
- Assuring the design of the process, both within the SIAM provider and with the suppliers
- Ensuring that the process interfaces to other processes work effectively
- Ensuring that there are effective process interfaces between different services and different suppliers
- Identifying potential service improvements for the process
- Managing service improvements for the process
- Supporting the Service Owners
- Managing the development, use, and improvement of policies, standards, and templates to support the process
- Managing the development, use and improvement of KPIs to support the process
- Managing the development, use, and improvement of capability and maturity assessments for the process
- Collating, anonymizing, and publishing benchmark reports in process capability and maturity across all service providers
- Being accountable for failures in the process, irrespective of which provider had the failure.

One useful approach is the establishment of a Special Interest Group (SIG) for each process, facilitated by the SIAM Process Owner and attended by the Process Owners from all suppliers. These SIGs promote collaboration between the suppliers, which is essential for effective SIAM. They should work together on specific developments, issues, and improvements that affect multiple suppliers. One example is an Incident Management SIG collaborating to create a standard definition of what information must be captured for an incident, in order to facilitate any flow of incidents between suppliers. SIGs are very effective in creating a collaborative and supportive culture in the supplier community, benefiting the overall delivery of services.

The following figure illustrates the peer to peer relationships that should be established between the process owners in the SIAM provider and the process owners in every supplier.

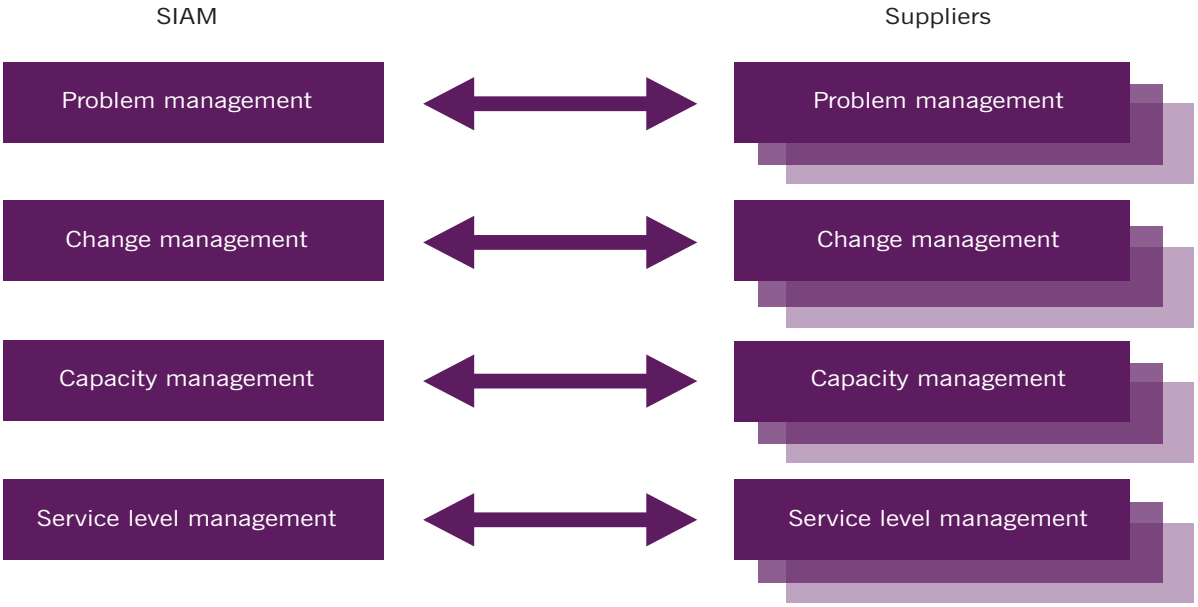

Figure 6.1 Example SIAM and supplier peer-to-peer relationships

6.2 SERVICE OWNERS

Establishing a network of service owners is critical to successful SIAM. They provide the necessary interfaces between the stakeholders within the business functions, the SIAM provider staff, and the suppliers. There should be Service Owners in the SIAM provider and in the suppliers.

6.2.1 SIAM Service Owners

Every business service should have an identified Service Owner in the SIAM provider. They are responsible for that service, and act as the single point of ownership for that service through the end-to-end SIAM model. They build relationships with the stakeholders for that service, and represent them within the SIAM provider and with the suppliers. One individual may act as the SIAM Service Owner for several business services.

Each SIAM Service Owner will also have relationships with all of the SIAM Process Owners, taking responsibility for ensuring that issues caused by the processes are addressed under continual service improvement.

There should also be identified Service Owner in the SIAM provider for each service line. The SIAM Service Owner builds relationships with the suppliers for the enabling services in that service line, and represents those suppliers within the SIAM provider and with the business. The SIAM Service Owner is responsible for driving evolution of the underpinning and enabling supplier services to support their business services. They also have responsibility for ensuring that the supplier's Service Owners progress continual service improvements related to their business service.

One individual may act as the SIAM Service Owner for several suppliers.

6.2.2 Supplier Service Owners

Every supplier, internal and external, should also have their own Service Owners for the services that they provide, with the same responsibilities as the SIAM Service Owner but within their own organization. These supplier Service Owners will have a relationship with the relevant SIAM Service Owners.

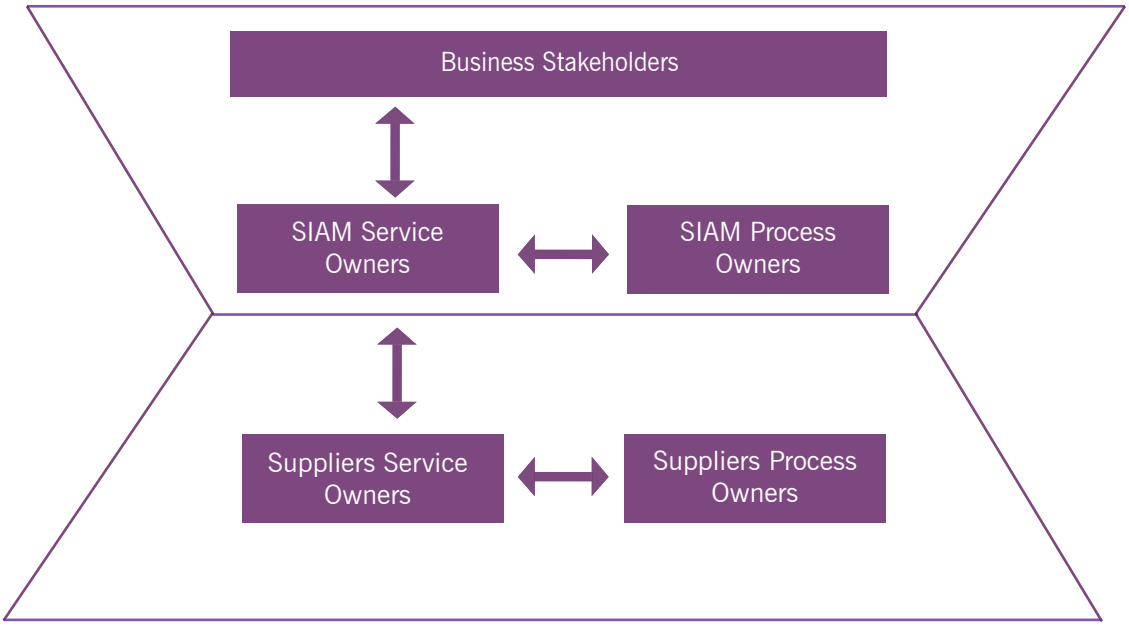

Figure 6.2 Service owner relationships

A SIAM Service Owner is responsible for:

- Relationship management with business stakeholders
- Relationship management with the suppliers Service Owners
- Overseeing all service improvements that affect their service
- Interfacing with the SIAM provider's process owners on issues and improvements
- Representing the users of their service on the ICAB
- Where allocated to a supplier, responsible for Service Level Management for the suppliers services.

A Supplier Service Owner is responsible for:

- Relationship management with the SIAM Service Owner
- Relationship management with the corresponding Service Owners in any subcontractors of the suppliers
- Relationship management with the corresponding Service Owners in other suppliers
- Overseeing all service improvements that affect their service
- Interfacing with the supplier's process owners on issues and improvements
- Representing their service on the ICAB
- Service Level Management for the services.

6.3 INTEGRATED CHANGE ADVISORY BOARD (ICAB)

The ICAB as described here is concerned with approving requests for change to put services live. Whilst a similar integrated approach should be used to approve developments and investments, this is not described here.

The ICAB performs the same function as any ITIL based Change Advisory Board (CAB) in reviewing and approving changes that are requested for deployment to live and pre-live environments.

It acts as the most senior CAB, and should only be concerned with changes that are of particularly high risk and/or impact, and which could affect the services from multiple suppliers. It provides the necessary controls for the end-to-end change management process.

The membership includes SIAM Change Management (from the multi-supplier co-ordination component), a representative from each supplier, and the appropriate Service Owners for the RFCs being presented to a particular ICAB meeting. The ICAB will only consider for approval or receive for information certain categories of requests for change. These are normally:

- Changes with high risk or high impact
- Changes that could affect the service provided by other suppliers
- Changes that the Supplier service provider wishes to be accepted as a Standard Change
- Changes that require a service outage to implement.

There should be a Change Policy (ideally developed by a multi–supplier Change Management Special Interest Group) that contains the guidance and policies to enable the identification of appropriate RFCs.

RFCs presented to the ICAB should already have been considered and locally approved by the suppliers own change management process. Once approved, the service provider should use the following approach to determine if the RFC needs to go to the ICAB.

6.3.1 Assess impact and probability

The RFC should be assessed using a matrix that is common across all service providers against:

- Impact to users (service consumers) of a failed change (failure during implementation and post implementation
- Probability of failure.

This will then give a numerical score for the RFC.

Impact					
High					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Low	1	2	3	4	5
	Low				*High* Probability

Table 6.1 Change impact/probability matrix

The score from the impact and probability assessment is then used to determine the category (Minor, Significant, Major).

Impact/probability score	Change category
1–4	Minor
5–15	Significant
15–25	Major

Table 6.2 Change categorization

The Category description should be used consistently by the SIAM provider and by all suppliers to provide common definition and understanding. It is worth noting that a change which is considered to be 'major' within a particular supplier may come out with a lesser category when considered within the whole SIAM environment, and vice-versa. This is perfectly acceptable, as long as the SIAM category is used in communications with the SIAM provider and with other suppliers.

6.3.2 Establish the approval level

The category is then compared against a matrix to establish if:

- The RFC needs no further approval
- The RFC needs to go to the ICAB for approval; or
- The RFC needs to go to the ICAB for information only.

This depends on several factors:

- Will the change impact be restricted to the suppliers own services
- Will the change impact or risk impacting services from other suppliers
- Will the change require an outage, or is there a high risk of an outage.

Change category	Impacts the suppliers services only	Impacts other suppliers services	Local but outage required or likely
Minor	Local approval	ICAB approval	ICAB info only
Significant	Local approval	ICAB approval	ICAB info only
Major	ICAB approval	ICAB approval	ICAB approval

Table 6.3 ICAB determination

Suppliers may choose to collaborate with other suppliers on local change management, including assessment and acceptance of the impact of a deployment, before presenting to the ICAB. This is acceptable, and suppliers should be encouraged to do so. However, the SIAM provider should retain the overall accountability and assurance.

The concept of standard changes can also be used for low risk, repeatable changes. The supplier should apply to the SIAM provider for a change of this nature to be approved and recorded as a SIAM standard change. Subsequent deployments of SIAM standard changes do not need to go to the ICAB.

Every supplier is responsible for:

- Local change management process
- Assessing RFCs for ICAB presentation after their own internal approval
- Submitting appropriate RFCs to the ICAB
- Presenting the RFC at the ICAB
- Attending the ICAB
- Reviewing and commenting on other suppliers RFCs that they believe could risk their service
- Addressing any issues raised at the ICAB
- Submitting requests for SIAM standard changes.

The SIAM provider is responsible for:

- Arranging and chairing the ICAB
- Circulating received RFCs
- Approving RFCs
- Pending RFCs until the next ICAB if not approved
- Communicating approved RFCs
- Approving SIAM standards changes.

6.4 R&MP

R&MP stands for Release and Maintenance Planning. It provides a single top level forward view for users, stakeholders, the SIAM provider, and suppliers of all planned releases and maintenance activities that will affect service, or have a high risk of affecting services. This helps to highlight and provide early awareness of:

- Planned outages
- Releases that are likely to affect other suppliers
- Releases that have a high risk of affecting other suppliers
- Conflicting dates
- Periods of very high release activity where the aggregation presents a high risk / impact to the business.

The Release and Maintenance Plan should include all tentative activities that have not yet had an RFC raised for them, as well as forward planned activities that do have an associated RFC. In this context, Releases should also include significant deployment activities.

This is not the same as a Change Schedule, as it does not include all changes. It is similar to the Projected Service Outage document, but it also includes activities that have a high risk of impacting availability.

The purpose is to provide a consolidated forward view for the SIAM provider and for all Suppliers, in order to:

- Assist in the early planning for integration and regression testing
- Identify potential clashes of release dates
- Identify compound risks with several activities planned for the same period
- Provide users with a forward view of potential service disruptions.

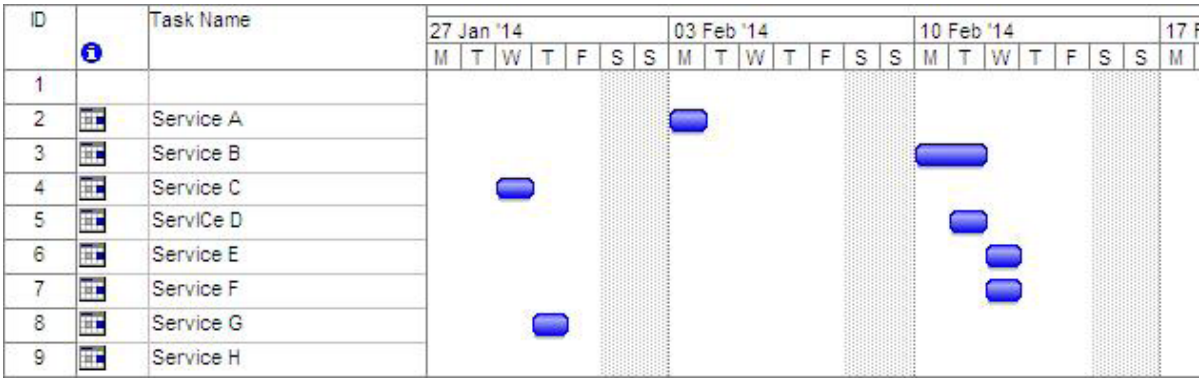

Figure 6.4 Sample R&MP plan

The horizon for the plan should be as long as possible. Suppliers should be encouraged to provide their tentative plans before they are firmed up, allowing sufficient time to re-plan if clashes are identified. Where possible, contracts should include the obligation for suppliers to maintain and provide a rolling 53 week forward view of major releases, maintenance activities, and deployment activities.

The information should be provided to the SIAM provider for collation on a periodic basis, dependent on the frequency of activity across the service providers. Weekly is recommended. A meeting is then held where suppliers can discuss potential issues with other suppliers. The SIAM provider is there to arrange and broker, responsibilities for identifying issues are with the suppliers.

Every supplier is responsible for:

- Providing the forward view
- Identifying and highlighting potential clashes and issues.

The SIAM provider is responsible for:

- Collating the information received from the service providers
- Communicating the combined plan
- Facilitating the R&MP meeting.

The SIAM provider also has the authority to request a re-schedule of activities, although the preference is that the suppliers discuss and agree this between themselves without having to escalate to the SIAM provider.

6.5 SERVICE BRIDGE

The Service Bridge provides a single point of escalation, communication, and management for high severity incidents ('major incidents') that occur in any of the services under SIAM governance. This should also include Security Incidents and Safety Incidents, even when the resolution of these requires the involvement of specialist SIAM providers such as Information Security (see chapter 3.2.5).

The purpose is to provide:

- Consistency in communicating the occurrence, status, and closure of high severity incidents to users and stakeholders
- A single point of management for high severity incidents that involve multiple Suppliers
- The ability for the SIAM provider to be fully aware of all high severity incidents
- Consistency in alerting business stakeholders
- Consistency in escalating to senior staff in the SIAM provider
- Providing a single point for senior stakeholders to contact for a status report
- Ability to provide management reporting on high severity service incidents in a consistent way.

Every supplier is responsible for:

- Alerting the Service Bridge for every high severity incident (as defined in the common standard for incident severities)
- Providing status updates to the Service Bridge at agreed intervals
- Managing resolution with their own teams
- Taking part in technical calls with other suppliers to jointly investigate live high severity incidents
- Attending any necessary management calls to provide updates and agree next steps to manage the resolution of live high severity incidents.

The SIAM provider is responsible for:

- Communication to stakeholders using different methods, for example:
  - Service status webpage
  - SMS texts
  - emails
  - Twitter.
- Monitoring the end-to-end service experience
- Managing the coordination of suppliers major incident teams
- Escalating to senior SIAM provider staff using a pre-defined and agree escalation path
- Escalating security incidents to the Information Security team
- Managing the suppliers provision of High Severity Incident Reports once the incident is resolved, detailing what happened and what actions are being taken to prevent re-occurrence
- Providing management reports on high severity incidents.

Staff allocated to the Service Bridge can also progress resolution of Problems with the suppliers when not working on major incidents. These are typically problems with a higher severity, or problems that span multiple suppliers.

6.6 SERVICE REPORTING

The goal of service reporting is to provide periodic consolidated reports to users and business stakeholders on the historic performance of all of the services against service levels. It aims to provide the information for different services in a consistent format, providing:

- Comparison of SLA achievement across different services and different suppliers
- One place for publishing all reports from all suppliers.

Period	Service	Supplier	Target availability %	Actual availability%	3 month trend
01/15	Email	ABC	99.87	99.88	Stable
01/15	Networks	DEF	99.5	99.4	Improving
01/15	Hosting	GHI	99.5	98.2	Declining
01/15	Hosting	JKL	99.95	100	Stable
01/15	Payroll	MNO	99	99	Stable
	Overall user experience		99.95	99.94	Stable

Table 6.4 Consolidation service report

Every supplier is responsible for:

- Providing service reports at the agreed time
- Providing service reports with the agreed information.

The SIAM provider is responsible for:

- Verifying the validity of service reports
- Collating service reports from multiple suppliers
- Publishing and communicating the consolidated service reports.

The reports should present factual information. This supports a culture where these consolidated reports can be published to all users of the services and all suppliers, without specific confidentiality agreements.

Reports typically include information sourced from multiple datasets, consolidated into a single validated and consistent set. Information is typically presented by:

- Service
- Supplier
- Customer (location and function).

Aggregated views are also created at different levels to provide appropriate levels of summarization for different levels in the organization, e.g. operational, tactical, strategic.

In the most mature of SIAM operations, this reporting aligns not just to the supplied services, but also to the business processes and services that those capabilities support. This mature reporting typically attributes financial value to the impact of service failures and disruption, alongside business impact such as lost business hours, number of customers affected, and financial implications such as lost business.

6.7 SERVICE INTRODUCTION

The SIAM provider must have an effective and consistent process and resources for introducing retiring, and replacing new services, new suppliers, and major changes to services. The process should use the full service lifecycle, with involvement commencing at the Strategy stage. This is often referred to as Service Introduction, and is the primary function of the Service Transition Planning and Support SIAM component.

Service Introduction is responsible for:

- Establishing the risk of the release
- Managing and addressing the risks
- Providing a summary of the outstanding risks to the ICAB for consideration when approving go-live
- Designing and using a controlled Gateway approach to approve moving into the next lifecycle phase dependent on achievement of defined criteria and open risks
- Maintaining and improving a master list of requirements and acceptance criteria for each ITIL process area
- Providing overall management through the lifecycle stages
- Ensuring readiness of the SIAM provider, suppliers, and users
- Working with functions outside the SIAM provider, such as systems integration
- Collating all the information to support service acceptance.

The approach must be flexible enough to cope with all types and sizes of new services/suppliers, using a risk based approach to agree which requirements and acceptance criteria are appropriate for each case.

When a new supplier is being introduced, the activities should include:

- Reviewing the supplier's processes, capabilities, and services against the operating model to establish any necessary changes to the models and processes of the SIAM provider, the business, the supplier, other suppliers, and the interfaces between them
- Designing and agreeing comprehensive service acceptance criteria
- Identifying any changes to tooling
- Identifying and resource implications
- Creating the Service Design Pack
- Managing the implementation and testing of any identified changes and additions
- Educating the supplier on the operating model
- Managing all necessary activities.

Service introduction will typically involve all of the SIAM components. This is a significant topic in its own right that merits its own White Paper.

6.8 SERVICE PORTFOLIO/CATALOGUE MANAGEMENT

The SIAM provider must have a service portfolio and service catalogue that describes all of the IT services that are under the governance and management of the SIAM provider and the business services that are provided to users.

These must be mapped so that dependencies between services are clear. They must also contain all of the information that the SIAM provider needs to do its job, for example the supplier name, contact details, hours of service. They should not contain any information that the supplier does not need to do its job. There can be multiple views of this portfolio and catalogue for specific stakeholders and consumers, however in order to maintain consistency the information must reside in a single portfolio and catalogue under SIAM change management.

The SIAM provider must also hold the catalogue of services that users can request from individual suppliers and from the SIAM provider.

Each supplier should also have their own service portfolios and catalogues for the services that they provide. These should also include dependencies between services, including services provided by other suppliers. They must also contain all of the information that the supplier needs to do their job. The level of detail and number of attributes is likely to be higher than in those held by the SIAM provider, for example the internal escalation contacts within the supplier.

This approach will result in duplication of some information between the SIAM provider and the suppliers, maintenance should be managed using a change management process. The effort for this is much less than the effort and loss of flexibility that would result in there was a single service portfolio and single service catalogue that included the full detail of all services from all suppliers.

The SIAM service catalogue should also include entries for each component provided by the SIAM provider. These should include information such as:

- A description of the service provided by the component (e.g. multi-supplier coordination)
- Any rate cards if the service is chargeable (notional charging is common in SIAM models)
- Hours/days when the service is available
- Metrics such as service levels, KPIs and Critical Success Factors
- Resource profiles for use in capacity management
- Any known constraints.

6.9 CONFIGURATION MANAGEMENT

The SIAM provider should maintain a configuration management system (CMS) that holds information on all the configuration items that it needs to perform its role. This will, of course, contain details of the IT infrastructure used by the SIAM provider's staff.

There may not be a need to hold detailed information of the individual IT assets that every external supplier uses to deliver their services, unless the SIAM provider requires this information to support the processes that it executes. For these services that are provided externally, the CMS maintained by the SIAM provider will typically only need to hold information on the following:

- The business services
- The services provided by the suppliers
- The suppliers
- Details of interdependencies and interfaces between services and suppliers
- SIAM component and process information
- Information on roles including process owners and service owners.

6.10 CAPACITY MANAGEMENT

In a SIAM model, the SIAM provider has responsibility for performing business capacity management. Its role is to collate and translate forecast user demand, and provide that to the individual suppliers. They are then responsible for component capacity management. Service capacity management is a joint responsibility of the SIAM provider and the suppliers.

The SIAM provider needs to create and maintain an effective model to capture and map the business forecasts to service capacity, ensuring that all suppliers have sufficient information to be able to plan for sufficient capacity. Forecasts against actuals should be regularly reviewed with the suppliers for all services so that the model can be used to ensure that sufficient capacity is available.

6.11 STANDARDS AND TEMPLATES

Where possible, the SIAM provider should work with the suppliers to define and implement standard templates to assist the interchange of information between the SIAM provider and the suppliers, and between the suppliers themselves. Specific examples are:

- **Severity levels**: common definition so that all suppliers, the business, and the SIAM provider have consistent understanding of severities, e.g. Severity 1 = system outage
- **Minimum incident datasets**: standard fields that all suppliers must use to record incidents, to assist the flow of incidents to and from suppliers. E.g. reporting user contacts, service ID, error messages. These can also be tailored for specific types of service to capture information specific to those technologies, e.g. IP address for network services
- **Capacity information**: standard template for exchanging capacity information between the SIAM provider and suppliers, including forecasts and actuals
- **Change information**: standard set of headings for exchanging information about changes eg Outage length, back-out plan, training requirements.

7 Further development of SIAM models

The model described in this White Paper is just one example of an effective model for SIAM. It is primarily a one dimensional model, where the SIAM provider can obtain specific behaviours from most suppliers, and where the SIAM provider is providing its services to one business customer.

Two dimensional models are more complex, but can support situations where a SIAM provider provides its services to multiple businesses, or where the SIAM provider is also involved in direct service delivery. Suppliers may also need to design their processes so that they can take part in multiple SIAM models.

8 Key definitions

The following terms are used throughout this publication.

Business in this publication is the organization that commissions the SIAM provider. The ITIL term 'customer' is deliberately not used, as in SIAM models the customer who buys an IT service may be a different organization to the one that pays for the SIAM provider.

Governance in this publication is the application of techniques for evaluating, directing and monitoring to deliver the agreed levels of service and meet business and corporate requirements.

Service Integration is a set of practices and an accompanying model and approach that adapt and augment the guidance in the ITIL publications for managing, governing, and coordinating the delivery of services provided by multiple suppliers (internal and external to the business organization).

Service Integration and Management has the same meaning as Service Integration.

Service line is a term used to describe a grouping of services under SIAM management and governance, grouped by either business function type (business service line) or technology type (technology service line). Defining and maintaining services, service boundaries, and service lines is part of the key to effective SIAM.

Service Management is responsible for managing the delivery of IT services from within a Service Provider, as described in the core ITIL publications. Within this publication this is also referred to as Operational Service Management.

Service Provider is an organization or team providing one or more specific IT based services to the business. It can be either internal or external to the business organization. The term 'supplier' is used synonymously in this publication for brevity. This also re-enforces the concept that within SIAM models a supplier can be an organizational unit within a business, not just an external service provider.

SIAM is a term that is used as an abbreviation for Service Integration and Management, and is also used to describe a service capability for Service Integration and Management, or a function or organization providing that capability.

Systems Integration is responsible for getting solutions, differing technologies, applications, and infrastructure to work together, with a focus on technology integration. Implementation of SIAM models often requires some element of Systems Integration, but it is important to understand the differences between the two definitions. Techniques for Systems Integration are not described in this publication.

Tower is a term often used to describe a set of services typically determined by technology type or by specific applications, provided by one or more suppliers, e.g. a Mainframe Tower which provides applications that run on a particular mainframe technology. It is preferable in a SIAM context to use the term 'service' rather than Tower, as SIAM models can be applied to any grouping of services, irrespective of any technology.

9 Benefits from using this model

Adapting to using this SIAM model is a business change. The benefits of this change are precisely the same as the benefits of any other business change that provides a consistent approach for a particular set of activities, e.g. consolidation of finance teams across a diverse business, standardising to use the same processes and tools.

These include:

- Optimized overall costs of providing the services to the business
- Reduced risks to the business
- Economies of scale
- Improved customer satisfaction
- Consistency of management, governance, and controls
- Improved quality of service to users
- A single point of ownership, visibility, and control of services
- Clearly defined roles and responsibilities
- Consistent use of quality processes
- Best use of skilled (and often scarce) resources
- Removed duplication of effort
- Ability to support changes to the supplier landscape
- Improved organizational capability and capacity
- Improved value of the services
- Increased responsiveness to change.

Specific benefits from using this SIAM model are most evident in areas including:

- Supplier contract optimization
- Consistent supplier performance management
- Robust cost management
- Clear ownership of incidents and problems
- Improved incident resolution times
- Improved service availability
- Consolidated service reporting
- Multi-supplier governance
- Multi-supplier coordination
- Effective introduction of new and changed services.

These are achieved through outcomes including the following:

- The creation of a homogeneous SIAM service capability
- Design, implementation, and use of this consistent SIAM operating model
- Designing for flexibility in the ability to manage a variety of existing and new services
- Delivering best balance between quality and lowest total cost of ownership.

Specific examples of additional benefits include:

- An improved understanding and overall reduction in service related risks to the business
- Clear ownership of major incidents and problems where the causing supplier is unclear (the well known ‘bouncing problem’, where no supplier accepts responsibility)
- A holistic model for capacity planning, linking business demand with supply from all suppliers
- The ability to compare and contrast the performance of services against service levels across multiple suppliers
- Mechanisms to highlight potential impacts of one suppliers release on another suppliers service, before any user impacts are experienced
- One place for users to understand in a consistent format the projected availability and status of all of the services, irrespective of who is the supplier.

End notes

1. 2006 Gartner Inc., Research Paper ID Number 600141795

Acknowledgements

Dave Armes, Daniel Breston, Niklas Engelhart, David Heaslet, James Finister, Peter McKenzie, Ivor Macfarlane, Steve Tuppen.

About the author

Kevin Holland is an experienced service management practitioner with a reputation for practical advice that extends the theory. For the last 10 years he has been actively involved in designing, implementing, improving, and advising on Service Integration and Management for a wide range of organizations in the public and private sectors. He is also active in developing service management qualifications.

About AXELOS

AXELOS is a joint venture company, created by the Cabinet Office on behalf of Her Majesty's Government (HMG) in the United Kingdom and Capita plc to run the Global Best Practice portfolio. It boasts and already enviable track record and an unmatched portfolio of products, including ITIL®, PRINCE2®, and RESILIA™ – the new Cyber Resilience Best Practice portfolio.

Used in the private, public and voluntary sectors in more than 180 countries worldwide, the Global Best Practice products have long been associated with achievement, heightened standards and truly measurable improved quality.

AXELOS has an ambitious programme of investment for developing innovative new solutions, and stimulating the growth of a vibrant, open international ecosystem of training, consultancy and examination organizations.

Developments to the portfolio also include the launch of PRINCE2 Agile™, the ITIL Practitioner qualification and a Professional Development programme, fully aligned to AXELOS Global Best Practice, for practitioners.

Latest news about how AXELOS is 'Making organizations more effective' and registration details to join the online community can be found on the website www.AXELOS.com. If you have specific queries, requests or would like to be added to the AXELOS mailing list please contact Ask@AXELOS.com.

Trade marks and statements

AXELOS, the AXELOS logo, the AXELOS swirl logo, ITIL, PRINCE2, MSP, M_o_R, P3M3, P3O,

MoP and MoV are registered trade marks of AXELOS Limited. PRINCE2 AgileTM and RESILIA™ are registered trade mark of AXELOS Limited.

Reuse of any content in this White Paper is permitted solely in accordance with the permission terms at https://www.axelos.com/policies/legal/permitted-use-of-white-papers-and-case-studies.

A copy of these terms can be provided on application to AXELOS at Licensing@AXELOS.com.

© Copyright AXELOS.

Our White Paper series should not be taken as constituting advice of any sort and no liability is accepted for any loss resulting from use of or reliance on its content. While every effort is made to ensure the accuracy and reliability of the information, AXELOS cannot accept responsibility for errors, omissions or inaccuracies. Content, diagrams, logos, and jackets are correct at time of going to press but may be subject to change without notice.