SIAM ITIL processes considerations

Extract from ITSM Zone material

Complexity

- In a SIAM ecosystem, processes can seem more complex due to factors including:
-
  - Different layers have different accountabilities and responsibilities within the same process
  - An increased number of parties is involved in end to end process execution
  - The need to integrate different processes from multiple organizations to support the end to end process
  - The number of interactions between processes from different organizations

- Complex processes are more difficult to understand and follow. Wherever possible, processes in a SIAM ecosystem should be designed to avoid complexity

Who owns the processes?

- Defining process ownership and levels of accountability and responsibility will also be important in a SIAM ecosystem. Common factors here include:
  - The customer is ultimately accountable for the outcomes of the processes, as they are the organization that commissions the SIAM ecosystem
  - The service integrator is accountable for:
    - The overall design of the process models, supporting policies, and data and information standards. They must ensure that the design will deliver the required outcomes
    - Their own local processes and procedures
  - The service providers are accountable for the design of their own local processes and procedures, ensuring that they comply with the process models, supporting policies, and data and information standards provided by the service integrator

Toolset

- The toolset(s) that will support processes need to be defined as part of the SIAM model. The decision about which toolset will be used and who will own it will be made during the Plan and Build stage of the SIAM roadmap.
- Decisions need to be made about:
  - Which toolset(s) will be used
  - Who owns the toolset(s)
- The outcome of these decisions will be documented in the tooling strategy. The decisions can only be made once the SIAM model has been finalized.
- If the customer owns the toolset, it will make it less challenging to change the service integrator. Alternatively, using a toolset owned by an external service integrator might offer an opportunity to access a best of breed toolset.

Data and information

Who Owns the Data?

- This decision needs to take into consideration what happens if a service provider or a service integrator is replaced. The customer organization should aim to have ownership of, or guaranteed access to, any data that is necessary to operate the services; for example, incident records.

Who Owns the Intellectual Property on Artefacts?

- As part of normal service operation in a SIAM ecosystem, artefacts will be created; for example, knowledge articles in the knowledge management repository.

- Intellectual property rights for these artefacts need to be defined and agreed in contracts or service agreements. There will be commercial considerations to take into account, for example, a service provider may be unwilling to share their articles with another organization.

Data and Information

Is data and information consistent?

- The SIAM model should include standards for data and information, and supporting policies. A data dictionary will ensure all parties use common standards.

- For example, there should be a minimum dataset for incidents and a standard definition of incident priorities and severities.

How is Access to Shared Data, Information, and Tools Controlled?
Policies and processes for access control need to be defined and managed, taking into account security considerations.

Process improvement

Who is responsible for process improvement?

- All parties in the SIAM ecosystem are responsible for improving their own processes, and for improving the end to end processes, facilitated by the service integrator.

- The service integrator is responsible for ensuring that the processes from different service providers continue to work together within the overall process models.

- The service integrator's process owners are accountable for end to end process improvement.

Compliance and assurance

- Compliance and assurance requirements should be included in contracts so that they can be enforced.

- The service integrator is accountable for assurance of process outcomes across the end to end processes.

Service Portflio Management

- It is not possible to transition to a SIAM model without a clear definition of all services, service providers, dependencies and relationships between services, and service characteristics. Service portfolio management information is therefore critical to any SIAM implementation
- The customer organization should own the service portfolio. Responsibility for execution of the service portfolio management process can be given to the customer's retained capabilities, or delegated to the service integrator
- The portfolio needs to be kept current with information from all service providers, including potential new services arising from innovation opportunities. Service provider contracts need to include a requirement to provide this information
- Data and information standards for portfolio records need to be agreed and consistent across all service providers
- The service portfolio management process must be aligned with the processes for introducing and retiring new services and new service providers

Monitoring and measuring

- Assuring the ability of all service providers to monitor their services and underlying technical components
- The requirement for a data dictionary, data models, terminology, thresholds and reporting schedules that are consistent across the SIAM ecosystem
- Shared performance measures to enable end to end reporting

Event Management

- The organizational design should include the function responsible for managing events. This could be a central function provided by the service integrator, a virtual function provided by all service providers, or individual functions in each service provider
- The rules for managing event thresholds should be defined in a policy that is consistent across all service providers; for example, at what point do repeated events concerning slow performance result in an incident being raised
- Specific tools may be required to collate events from multiple service providers, correlate the data, and apply rules to identify end to end issues
- Targets for event diagnosis and resolution should be common across service providers

Incident Management

- The incident management process model needs to support prompt restoration of service. This includes routing incidents to potential resolvers as quickly as possible, and with the minimum number of parties involved. The associated service desk model needs to support this
- Data and information standards for incident records, incident transfer, and supporting tooling must be defined, to support the effective referral of incidents between service providers
- Incident priorities and severities should be defined consistently across all parties
- Roles and responsibilities must be defined for coordinating incident investigations that involve multiple service providers
- Targets for incident resolution need to recognize that incidents may be referred between service providers. The referrals will take time, and each service provider will have their own agreed targets. The end to end process needs to make sure that customer targets are not breached, even if every provider achieves their own target
- There is a risk that service providers may refer incidents to another service provider to avoid breaching a resolution time service level
- Incident management teams from different providers are likely to be in different geographical locations, creating challenges for collaboration on incidents

Problem Management

- Getting all parties to take part in problem management working groups and forums, including joint working to resolve problems that involve multiple service providers
- Coordinating problem investigation and resolution activities across multiple service providers
- Encouraging and facilitating the sharing of data and information on problems with other service providers
- Aligning targets for problem resolution across service providers
- Creating and using common terminology, data and information standards, and problem classifications across service providers

Change Management

- The scope of change management needs to be clearly defined. The process can encompass many areas, including:
    - Technology
    - Processes
    - Policies
    - Organizational structures
    - The SIAM model
- Common standards should be developed for data and information and included in a change policy. For example, types of change, approval levels and notice periods
- The roles and parties involved in reviewing and approving changes must be clearly defined, and should include all organizations who may be affected by the change
- Consideration should be given to:
  - Having different reviewers and approvers for different types and classes of change. Who approves a change should depend on risk and impact, and if the change is an emergency
  - Allowing service providers to approve their own proven low risk, repeatable changes that don't affect other service providers
- Leveraging automated testing and deployment techniques to reduce the level of manual review required and improve change success rates

Release Management

- Release planning and implementation needs to consider all the affected service providers, and the customer organization. This includes coordinating and scheduling releases to avoid negative impact
- Responsibilities for testing integration between services from different service providers should be defined
- There should be a consistent format and method for communicating information about releases

Configuration Management

- The scope of the service integrator's CMDB must be clear, and should only contain data that the service integrator needs to fulfil its responsibilities
- Service provider contracts and agreements need to stipulate what configuration management data they are required to provide
- Each organization is responsible for maintaining its own CMDB, containing the data necessary to support delivery of its own services
- Service providers need to share a subset of the data in their CMDB with the service integrator and other service providers, to support delivery of the end to end service
- A policy should be defined to specify common classifications and record contents for any configuration data that needs to be shared across parties in the SIAM ecosystem
- The approach, toolset integration, and access control for sharing CMDB data between different parties needs careful consideration
- Where CMDB data is shared, responsibility for maintaining shared items must be defined
- Responsibilities for assessing and improving data quality and CMDB accuracy should be defined

Service Level Management

- Service providers need to recognize that the service integrator is acting as the agent of the customer and work with them on SLM activities and reporting
- The scope of SLM should be clearly defined. Its activities need to be distinct from those of:
  - Supplier management
  - Contract management
  - Performance management
  - Business relationship management,

  even if performed in the same layer. The interfaces between these processes should be mapped
- SLM needs to include thresholds to define when a breach of performance should be escalated to supplier management, so the process can apply remedies
- The SIAM model needs to reflect any service level targets that may have been agreed before the service integrator was appointed
- The scope of the contracted services, and any dependencies on services from other service providers, must be clearly defined
- An approach must be established to manage the situation where the failure of a service provider to meet their targets is due to another service provider
- The service integrator will need information to verify the service providers' performance reports. This may need to be sourced from other service providers and from service consumers
- It can be challenging to produce consolidated reports unless the service level targets of all service providers are aligned. For example: a common definition and calculation of 'availability', and reports covering the same time periods
- Consideration should be given to including internal service providers within the scope of SLM

Supplier Management

- Supplier management is normally executed by the service integrator, acting on behalf of the customer
- Supplier management should be clearly defined as separate from contract management and service level management, even if performed in the same layer. The interfaces between these processes should be clear
- This process should manage service provider performance escalations received from the service level management process
- A supplier management policy should be created that is appropriate for and fair to different types and sizes of service providers
- The execution of the process should not favour one service provider over others. This can be a challenge if the service integrator is also a service provider, or where some service providers are internal
- There should be a clear definition for when the supplier management process can apply remedies, and when a breach of performance becomes a breach of contract that should be escalated to contract management
- A mechanism should be developed to apportion remedies for failure to meet service level targets where multiple service providers contributed to the failure
- Non-financial incentives can be as effective as financial remedies to drive appropriate service provider behaviour
- Supplier forums can assist in creating a collaborative culture

Contract Management

- The customer is always accountable for contract management; they hold the contracts with the service providers. Some organizations delegate responsibility for execution of some activities to an external service integrator, or use them as an advisor
- Contract management should be clearly defined as separate from supplier management and service level management, even if performed in the same layer. The interfaces between these processes should be clear
- A SIAM ecosystem requires appropriate contracts to avoid vendor lock in, provide for shared goals, shared risk and reward, end to end service levels and performance measures, collaboration, and the right of the service integrator to act on behalf of the customer
- Clearly define when a breach of performance becomes a breach of contract. This process is responsible for managing breaches of contract
- Ensure that contract breaches are addressed consistently and fairly with all service providers
- Implement practices to support management of multiple contracts, including a contract repository with associated access management