Governance in a Multi-Supplier Environment

This paper provides advice and guidance for organisations faced with governing a multi-supplier environment.

1. The Need for Governance

ISACA, the global IT governance association, defines corporate governance as:

> "The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives."

If we translate this into the scope and context of Service Integration and Management (SIAM) we can say that SIAM governance is:

> "The system by which an organisation directs and controls the integration and management of multiple suppliers. The board of directors is responsible for the governance of their enterprise, including ensuring that a system of appropriate controls is in place to govern the use and activities of suppliers. The system of governance consists of the leadership, organisational structures and processes that ensure that services are sustainable and meet objectives"

Virtually all organisations are now heavily reliant on their IT to support the operation of business services and facilitate achievement of business objectives. However today's organisations are also faced with a complex IT landscape, where significant rates of change occur, and security threats are constantly evolving. The risks that this perpetuates, necessitate the need to ensure that adequate Governance exists, and in many sectors there is now legislation aimed at ensuring this.

In part, the complexity of the modern IT landscape is brought about by the advent of cloud computing and the different 'as a service' models that organisations are increasingly making use of. While this is frequently sold as a way of making the provision of services 'easier', at this stage, it is typically increasing the overall number of suppliers that organisations are dealing with, and potentially adding complexity as different suppliers are now responsible for different layers of a service. In addition the ease with which the business can procure these services can often lead to the growth of 'shadow IT', with the expectation that IT will, when necessary, have the skills, understanding, resource and ability to support these services.

The need to ensure appropriate governance exists whether IT is primarily resourced 'in-house' or is 'out-sourced'. Even if the whole of IT is out-sourced, perhaps to a primary supplier, the organisation remains responsible for ensuring that risks are assessed and adequate controls in place.

2. The Scope of SIAM Governance

SIAM Governance is primarily focused on ensuring that:

- The SIAM Strategy and Operating Model meets the current and future business needs
- The SIAM Strategy and Operating Model are planned and implemented successfully
- The SIAM Strategy and Operating Model are managed and operated in a controlled manner, while being both efficient and effective

Within this paper the first two bullet points are considered under Strategic Governance, while the third bullet point is covered in the Operational Governance section.

It is extremely important at this point to note the difference between governing and managing (or operating) the SIAM operating model. Governing is the process of setting the direction, then implementing, maintaining and utilising the set of controls that serve to ensure that the organisation follows the intended course, with timely course corrections being made when necessary. Managing involves the allocation of resources and the day-to-day operation of the organisation. In this way it can be seen that strategic governance should always remain the remit of Retained IT, while managing the operation may, depending on the SIAM model deployed, be outsourced. In terms of operational governance, both the client organisation and the Service Integrator (where different) have an interest in ensuring that controls are in place and things are working according to plan, so responsibilities may be shared, as long as Retained IT have visibility and assurance that the necessary controls are in place and working.

When looking at the scope of governance we need to consider what there is that needs to be governed. At the strategic level we should include:

- SIAM strategy (implementation and maintenance of the strategy)
- SIAM model (the SIAM model that adopted by the organisation)
- SIAM plans (implement and operate plans)
- SIAM process architecture
- SIAM tooling strategy (including roadmaps)
- SIAM tooling architecture
- SIAM tooling plans (implement and operate plans)
- SIAM organisational responsibilities
- SIAM process and tool ownership
- Conformance with applicable external factors (e.g. laws and regulations)
- Conformance with applicable internal factors (e.g. organisational policies and standards)
- Strategic risks and controls
- Strategic SIAM documentation
- Service Management data

At the operational level we should include governing:

- Operation of the implemented SIAM strategy
- Supplier on-boarding, transition and off-boarding processes
- Process operational plans
- Process definition documentation (e.g. process scope, flows, descriptions, interfaces)
- Conformance with applicable policies and controls
- Process related roles and responsibilities
- Tool configurations and documentation
- Tool related roles and responsibilities
- KPIs and metrics for:
    - Service Integrator
    - Suppliers

- Processes and functions
- Operational reporting mechanisms
- Service improvement plans
- Operational risks and controls
- Audit policy, plan and schedule

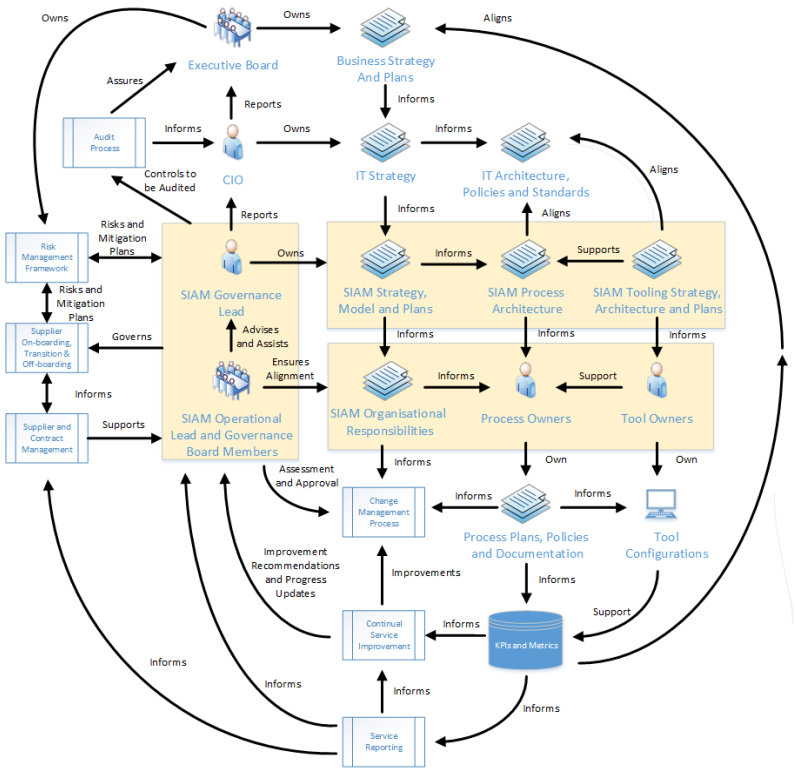
The SIAM governance solution needs to consider all of the above items and how they will be produced, maintained, recorded/stored, monitored and reviewed. Regular review and maintenance is important as over time business requirements and objectives will change and the SIAM strategy and/or operations will need to adapt accordingly.

3. A Framework for Governance

The diagram within this section shows an example SIAM Governance Framework, comprising of a range of components and the relationships between them. The various components are described within this paper and the relationships are intended to indicate where each component fits in and why it is important to the overall governance framework.

The diagram is not intended to be a 'one size fits all' SIAM Governance Framework, as this would not be practical nor advantageous. Virtually all organisations tend to be coming from an existing 'historical' position where some governance mechanisms will already exist, possibly in other forms or under other names. Different organisations will have different requirements in terms of the degree and formality of governance needed, driven by their own business requirements and applicable external factors such as legislation. Additionally, with governance in particular it is critical to take account of the organisation's size and culture, when considering the mechanisms to put in place. Trying to force an overly bureaucratic and rigid governance framework onto a smaller organisation that has a very informal culture, is unlikely to work, while another larger more formal organisation may actually expect additional controls.

This example SIAM Governance framework should act as a starting point, which can then be adapted by organisations to meet their specific requirements and terminology.



4. Strategic Governance

This section discusses strategic SIAM governance topics including:

- Roles and responsibilities
- Ownership
- Governance of documentation
- Monitoring implementation plan success
- Monitoring operational achievements against strategic objectives
- Tooling strategy
- Data segregation and ownership

Strategic Roles and Responsibilities

SIAM Governance Lead

This is a senior role within the Retained IT organisation, typically reporting into the CIO and responsible for providing assurance regarding the successful implementation and operation of the SIAM strategy. The role requires experience of governance, management, IT operations, IT project delivery, working with suppliers and Service Management, along with excellent communication skills in dealing with people at all levels within the organisation and externally.

During design and implementation phases the SIAM Governance Lead should work with the Programme Manager to ensure continued alignment between business requirements, IT strategy and the SIAM strategy and plans. Once operational, the SIAM Governance Lead will be responsible for working with all parties involved to ensure that the implemented SIAM strategy achieves its objectives. This will include representing SIAM within the greater organisation and communicating achievements and progress.

The SIAM Governance Lead owns the SIAM strategy, plans, the process architecture, and the SIAM tooling strategy, architecture and plans. The role is responsible for ensuring that these artefacts are maintained and remain aligned with business plans and the IT strategy.

The SIAM Governance Lead will chair the SIAM Governance Board and be responsible for its effective and sustained operation.

As with all roles, the role and its responsibilities should be documented and formally agreed.

SIAM Governance Board Members

A SIAM Governance Board should be established as soon as responsibilities for SIAM operations have been identified. The Board will be responsible for supporting the SIAM Governance Lead in ensuring that SIAM is implemented and operated in accordance with strategy and plans, that any changes to SIAM strategy or operations are properly assessed, any issues or risks understood and addressed, and any potential improvements identified.

The board should have representation from Retained IT, the Service Integrator (whether retained or outsourced) and key suppliers (both internal and external), and provide coverage across all key processes and functions. A cycle of regular board meetings should be established but board members should also be available when required to review, discuss and approve changes and actions outside the normal meeting cycle.

Ownership

Ownership is an important governance concept, as frequently activities such as the maintenance of documentation do not occur due to a lack of clear ownership. All of the documentation within the SIAM Governance Framework must have documented and agreed ownership.

Similarly, all the processes and supporting tools utilised by SIAM must also have clear and agreed ownership. In the same way as for documentation, a frequent reason for software tools not being maintained is due to them having no clear ownership. Assignment of ownership must be carefully considered as it is important that the ownership of both

processes and tools be an active role, which actually has some time spent on it, rather than a 'tick in the box' assignment of the role to someone who has neither time nor interest in performing the role. Here, budget, may also be a consideration as it makes little sense to assign the ownership of a tool to someone who has no access to any budget with which to maintain the tool. The tool owner may not necessarily be the budget holder but they should have access to the relevant budget via either a reporting line or other mechanism.

Strategic SIAM Documentation

There is a range of key strategic documentation that needs to be governed:

- SIAM strategy
- SIAM model
- SIAM implementation and operate plans
- SIAM process architecture
- SIAM tooling strategy
- SIAM tooling architecture
- SIAM tooling plans

In terms of governing this information, we need to ensure that:

- Formal review, approval and sign-off mechanisms exist and are followed
- The artefacts exist, have been documented and have been approved/signed off
- The artefacts take into account and comply with all applicable external (e.g. laws and legislation) and internal (e.g. organisational policies and standards) control requirements
- The information is readily available to those that need it and are authorised to see it, but restricted from unauthorised access
- Any changes to the artefacts are managed and tracked
- The artefacts are regularly reviewed and when necessary updated to ensure continued alignment with business plans and IT strategy
- Implementation and operation of the SIAM strategy, model, architecture and plans remains consistent and aligned with the documentation. Where this isn't the case we need to identify whether the activity needs to be corrected or the documentation updated

In order to provide this governance, the governance framework should include the following controls.

Change Management and Approval

There are two primary reasons why Change Management is important to the governance of the strategic SIAM documentation:

- The information within the SIAM Governance documents needs to be controlled to prevent unapproved (and perhaps ill-considered) changes. Any changes need to be considered for impact across all processes, functions and key suppliers, which is where the SIAM Governance Board comes in
- Any significant business or IT changes outside of the SIAM Governance Framework, need to be considered for possible impact on the SIAM strategy and the operation of that strategy

Although ITIL states that key documentation should be within the scope of the Change Management process, this does vary from organisation to organisation and currently many do not typically include documentation changes within their process scope. Where possible it makes sense to do so, as in Change Management we have a process that includes assessment, approval and notification of changes, all of which we need to help govern the SIAM documentation. Core members of the SIAM Governance Board can be included as assessors for relevant changes.

However, if organisations already have other mechanisms for managing documentation changes, perhaps as part of a document management system, then this can be a viable alternative. In a smaller or less mature organisation, the mechanism may simply be a process of emailing the document to the SIAM Governance Board members,

incorporating comments and feedback, then following final approval by the relevant authority (such as the SIAM Governance Lead), placing the updated document into a controlled location. As long as the process is understood and provides adequate control, this may be acceptable at this stage in the organisation's evolution.

Document Management and Storage

Organisations will often have their own established mechanisms for the management, naming, labelling and storage of documents. Some will have fully specified document management systems with built-in approval workflows and document versioning, while others may just have some general policies for security marking documents and perhaps access to a SharePoint structure. Generally speaking, it is fair to say that the ability to locate, manage and control documentation could do with improvement within many organisations.

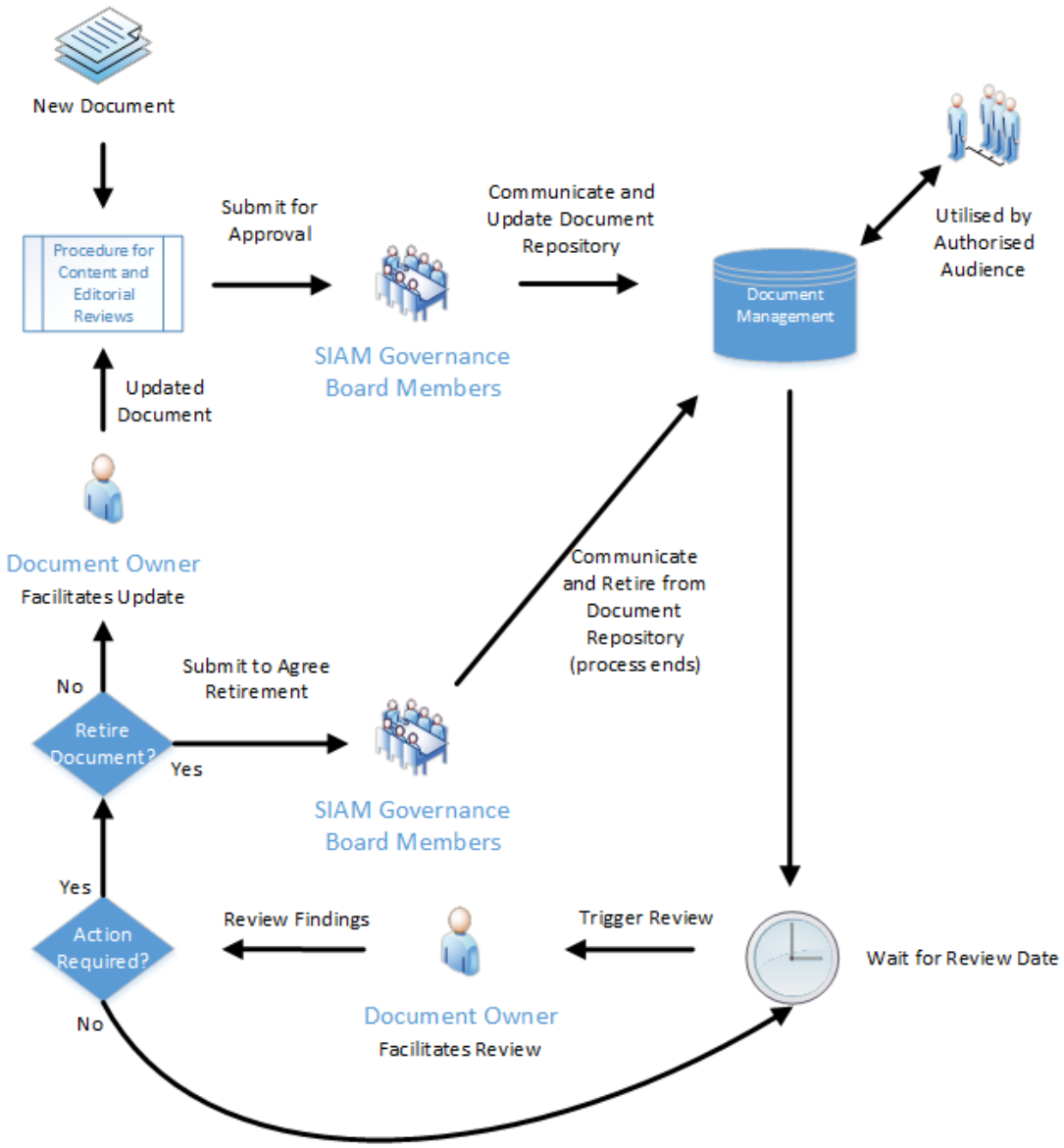
As such it is recommended that any SIAM programme, review the existing mechanisms and decide whether these should be utilised or a different solution put in place. The primary requirements for any solution should be that:

- Approved documents can be readily accessed by those needing and authorised to access them
- Unauthorised access is prevented
- Documents can be searched for and located
- Documents can be version controlled and changes tracked
- Document ownership can be recorded
- Documents can only be uploaded or amended by a controlled set of authorised individuals
- A process exists for assessing and approving new or changed documents

Strategic Review Cycle

There should be a strategic review cycle to ensure regular reviews (at least annual) of all key documentation to ensure continued alignment, relevance and accuracy. This process also helps ensure that document ownership is still correct.

The review should trigger the document owner to review the content and identify any changes that are now required. They should then manage the updating of the document and pass it into the approval process. An example process is shown below:



The document owner should also review and update the document between standard reviews, when they become aware of any changes that may impact the documented information. Due to this, it generally makes sense for the document owner to be involved in the subject matter, rather than assigning the ownership to an individual who is isolated from the material in question and who is thus unlikely to become aware of necessary changes.

Monitoring and Reporting

The SIAM Governance Board are responsible for monitoring progress and reports regarding implementation and operation of the strategy and associated plans. One aspect of this monitoring should be to ensure that actual activities are still aligned with key documentation. Where exceptions are identified, the board need to understand whether this is:

- A temporary, tactical change for a justifiable reason (which needs to be understood and monitored)
- An erroneous deviation perhaps due to misinterpretation of the documentation (which needs corrective action)
- An emerging change due to newly discovered information, external factors or evolving requirements, that needs to be assessed for impact and then plans (or other documentation) changed accordingly

Success of Implementation Plans

At the strategic level, the success of SIAM implementation plans needs to be tracked and monitored. During initial implementation or transition, this should of course be being done by the Programme Management staff, however once in role, the SIAM Governance Lead and the SIAM Governance Board should also be involved.

Following the initial SIAM programme, there may still be implementation plans underway at times, perhaps to bring in other process areas or new tools, and progress on these again needs to be monitored and communicated across the SIAM ecosystem.

Progress against key plans should be reviewed at SIAM Governance Board meetings, so that there is a common understanding of objectives, progress and timescales, and to allow a forum for discussion of any issues, impacts on related processes or potential changes to the plans.

The primary purpose of this activity should be to ensure that the implementation of the strategy is going according to plan and does not need corrective action in order to ensure that the intended objectives are met.

Operational Achievements against Strategic Objectives

Ongoing monitoring and review should also be carried out to understand whether the operation of the SIAM strategy is achieving (or on track to achieve) the intended strategic objectives. So, if one of the strategic objectives was to obtain £2M cost savings over a certain number of years, as part of governance we should be tracking against this objective to understand whether it has been or can still be achieved. In some organisations this value tracking may be occurring elsewhere, perhaps as part of Portfolio Management, but even if so, the SIAM Governance Board should be obtaining the information from them and reviewing it.

During the course of a programme and its value realisation, there may be changes of scope, business strategy, external factors (e.g. legislation) or priority, which necessitate the programme objectives being re-considered. Often a decision needs to be made as to whether to accept a programme change and alter the intended programme objectives accordingly, or reject the change (where feasible) and retain the original objectives. What should be avoided is allowing programme changes to occur but retaining the original objectives where they are no longer realistically attainable, hence setting up the programme to be measured as a failure.

Where the SIAM Governance Board identify, through regular monitoring and review, that operation of the SIAM strategy is not on track to meet the intended objectives, timely consideration needs to be given as to whether any corrective action can and should be implemented to bring the plan back on track.

Tooling Strategy

A SIAM tooling strategy needs to be developed, implemented and maintained. This should cover the Service Management and Systems Management related tooling requirements for all in scope processes, functions, platforms and services, as well as the integrations between different tools. In part, as should happen with any Service Management implementation, this is to aid cost effectiveness by preventing each area from going off and selecting their own tools (e.g. monitoring tools), which is likely to lead to increased complexity, license costs and support costs, the need for integration of disparate tools, duplication of both tool functionality and effort, and increased capacity requirements due to potentially having multiple clients on each system.

However, from a SIAM perspective this strategy is also required to establish how some of the technical aspects of service integration will be implemented. Often this strategy will have commercial contract implications, for example, will all suppliers be expected to use the Service Management toolset owned by either Retained IT or the Service Integrator? If suppliers are able to use their own toolsets and integrate with the Service Integrator's toolset, what are the rules around this? At what volume of traffic does an integration need to be automated rather than manual? If asset or configuration data is being fed by suppliers up to the Service Integrator, what is the required frequency, content, format and medium?

The tooling strategy, architecture and plans must be aligned with IT enterprise architecture standards and policies, and support the planned SIAM process architecture. Governance needs to exist to ensure that the tooling strategy is

developed, aligned, agreed, signed off and then owned and maintained. Governance should also be making sure that supplier contracts are aligned with both the SIAM process architecture and the tooling strategy.

Over time the tooling strategy will need to be updated and subject to continuous improvement, so ongoing ownership is critical.

Data Segregation and Ownership

Other strategic considerations, related to tooling and governance, are data segregation and data ownership.

In a multi-supplier environment, suppliers may be reluctant to share information such as costed quotes for planned changes, knowledge documents and current problems. Consideration thus has to be given as part of the tooling strategy, as to whether any data segregation will be employed.

In the case of common data, that may be utilised by a number of tools, the strategy needs to consider which tool will be the 'master' source of this data, which in turn will determine the direction of related data integrations. In secure environments, thought must also be given as to the type of information that is allowed to be held on different systems, for example it may not be permitted to hold hostname and IP address information within certain applications due to their placement or security classification.

Another consideration is data ownership. As time goes by, a wealth of information will build up within the Service Management tools, including past Incidents and Problems and how they were resolved, existing known errors, the history of changes made to the infrastructure, and capacity baselines and trends. When contracts end, perhaps with a move to a different supplier, who owns this data, and even if the retained organisation owns it, can it be handed over in a usable form if it was previously held within the Service Integrator's toolset?

In terms of strategic governance, it is important that the SIAM Governance Lead and the SIAM Governance Board members ensure that this strategic planning is occurring, with the decisions and the reasons for those decisions documented. Going forward the focus should then be on checking alignment with strategy and ensuring that the strategy is regularly reviewed and updated to maintain currency and relevance.

5. Operational Governance

This section discusses operational SIAM governance topics including:

- Roles and responsibilities
- SIAM organisational responsibilities
- Supplier on-boarding, transition and off-boarding
- Supplier and Contract Management
- Monitoring and review
- Process governance
- Document governance
- Operational review cycle
- Auditing
- Continual Service Improvement

Operational Roles and Responsibilities

SIAM operational roles include:

SIAM Governance Lead

The SIAM Governance Lead role within Retained IT should be responsible for monitoring and reviewing the operation of the SIAM strategy, with a focus on:

- Maintaining and operating the SIAM Governance Framework
- Ensuring that appropriate policies, processes and controls exist and are implemented consistently

- Ensuring operation is in line with strategy and strategic objectives
- Measurement and review of both Service Integrator and overall performance
- Continuous improvement of the SIAM ecosystem
- Efficient and transparent on-boarding, transition and off-boarding of suppliers

The SIAM Governance Lead must provide guidance and leadership as the chair of the SIAM Governance Board, and be responsible for the implementation and ongoing operation of the SIAM Governance Framework.

SIAM Operational Lead

The SIAM Operational Lead is a role that may exist within either Retained IT or the Service Integrator, depending on the division of responsibilities that the organisation decides upon. This division will be influenced by a range of factors including the levels of trust, Service Management maturity, complexity, and control required. Typically, this role may be performed by someone in the post of Head of Service Delivery, although this will vary between organisations.

The SIAM Operational Lead should be responsible for managing the day-to-day operation of the deployed SIAM model and ensuring that the process framework is operated effectively and consistently across the supplier landscape. To achieve this they must work with the different Process Owners and managers, function leads, and supplier representatives, to communicate plans and objectives, allocate resources, assist with the timely resolution of issues, build relationships and mitigate risks.

The role should work in conjunction with the SIAM Governance Lead to ensure that responsibilities for operational SIAM governance are defined, agreed and understood, and that necessary controls are implemented and working as expected.

The SIAM Operational Lead will be a key member of the SIAM Governance Board.

SIAM Governance Board Member

The SIAM Governance Board should act as a forum for the review, assessment and discussion of SIAM and Service Management related matters. The board members should support the SIAM Governance Lead and SIAM Operational Lead in governing the implementation and operation of the SIAM strategy, and be responsible for communicating SIAM strategy, plans and objectives within their own organisations and areas.

The board members should assess proposed changes to strategy, processes, plans and tooling, so that cross-process and cross-organisation impacts can be understood. For example, a change in the Problem Management process to do with how Problems are categorised, may seem a localised change, but actually may impact reports within Service Reporting, contracts within Supplier and Contract Management, and tooling integrations with respect to one or more suppliers.

Process Owners may be asked to update the board on current activities, achievements, issues and plans within their scope, especially where the process is new or has been having issues.

Process Owner

Process Owners play an important role in governing their own processes, as well as participating in the SIAM Governance Board where required. They should own the process documentation and make sure that the process roles are assigned, agreed, understood and being performed.

Each Process Owner should be monitoring their process to ensure that people are aware of it, following it and that efficiency, effectiveness and quality are at the required standard. They should own and drive continuous improvement plans for their process area, and liaise with other process areas to ensure interfaces are implemented and working as required.

Tool Owner

Similarly, Tool Owners also play an important governance role by providing ongoing ownership for a tool and acting as a contact point for any questions regarding the tool. The Tool Owner should own the tool roadmap, implementation/upgrade plans, configuration, integration specifications and any known issues, as well as being involved in any release planning and patching decisions.

Depending on the nature of the tool, the Tool Owner may also maintain the prioritised list of enhancement requests related to the tool and have access to a budget with which to maintain and, where agreed, further develop the tool configuration.

Supplier Manager

The specific role name tends to vary from organisation to organisation, but this is the role that manages the contract(s) with one or more suppliers. A great deal of the actual work with regards to SIAM can be related to getting the contracts right and then ensuring that both the contracts and the supplier relationships are managed properly. Having the Supplier and Contract Management staff on-side and actively involved in any SIAM implementation/transformation from the start, will pay dividends.

Supplier and Contract Management is an important part of the SIAM Governance Framework, and appropriate time and effort should be devoted to developing contract templates that are aligned with the SIAM strategy and cover all parts of the contract lifecycle including transition of work to another supplier at contract end.

Due to the importance of this role, the team should have representation on the SIAM Governance Board to ensure that contractual understanding and viewpoints are present during discussions.

SIAM Organisational Responsibilities

Once decisions have been made on the SIAM strategy and the SIAM model that is being adopted, the high-level responsibilities at each layer of the model should be documented and agreed. For instance, it may have been decided that a primary supplier will act as the Service Integrator, but now there needs to be further definition of exactly what Retained IT are going to remain responsible for, what the Service Integrator will do and what individual supplier towers will take on.

As well as determining where process ownership should reside, this exercise should also create a number of principles regarding organisational responsibilities, which will be used as input to process architecture design, detailed process design and tooling requirements, as well as contractual negotiations. Examples of these operating principles could include:

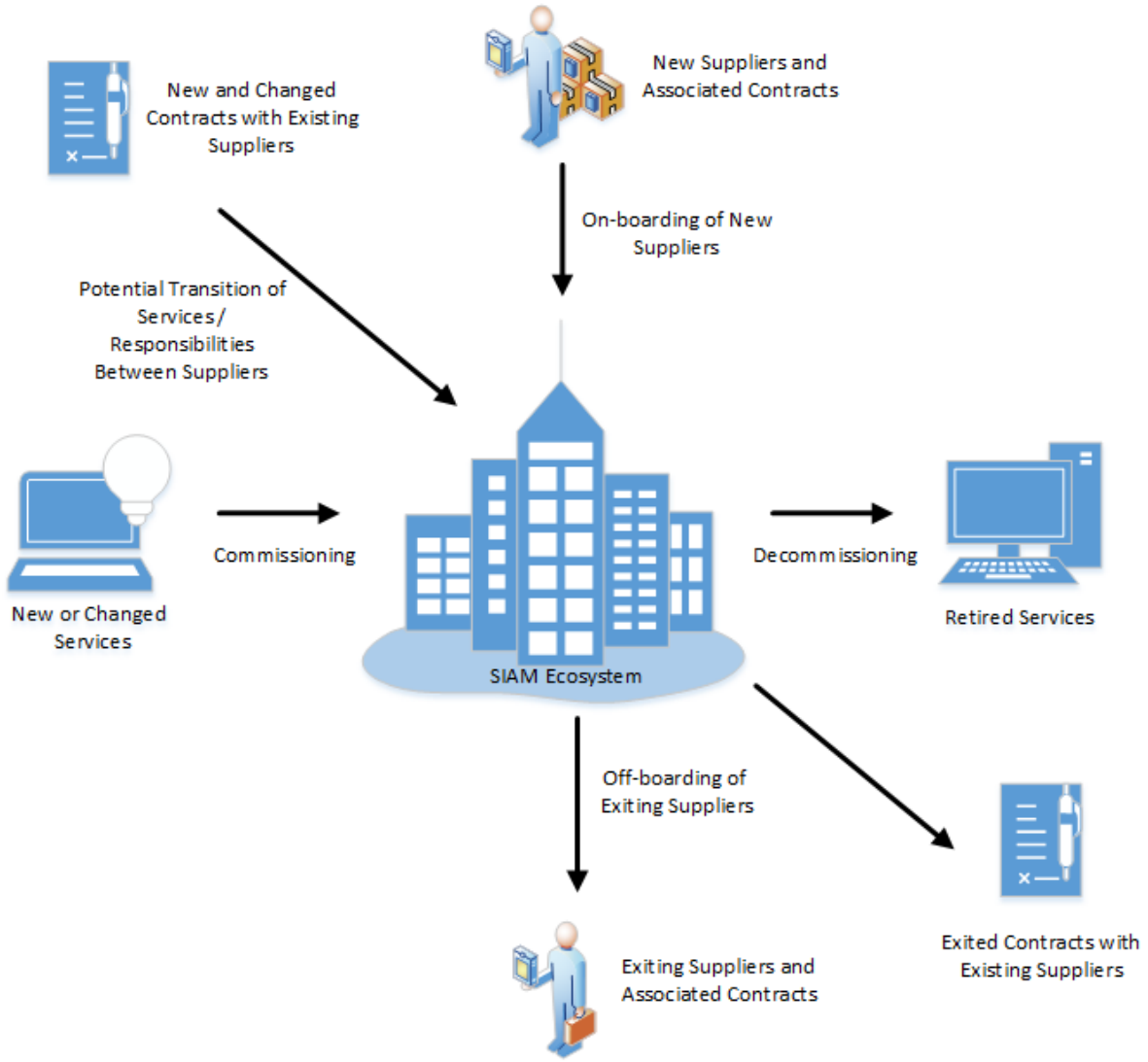
- All major incidents will be managed by the Major Incident Team within Retained IT
- Enterprise architecture will remain the responsibility of Retained IT
- All major and emergency changes must be approved by the Service Integrator
- The co-ordination of all cross-supplier changes will be provided by the Service Integrator

In terms of operational governance, we need to ensure continued alignment with these operating principles, or where necessary agree that a principle now needs to be changed.

To help govern this, within the SIAM Governance Framework we have the following components:

- Documented SIAM Organisational Responsibilities (operating principles)
- Change Management process (proposed changes can be assessed against the operating principles)
- SIAM Governance Board (responsible for assessing the impact of relevant changes and monitoring continued alignment to the organisational responsibilities)
- Supplier and Contract Management process (to help ensure that contracts are properly defined to support alignment to the operating principles)

Supplier On-boarding, Transition and Off-boarding



Over time new suppliers will need to be on-boarded into the SIAM ecosystem, existing work may need to be transitioned to alternative suppliers and previous suppliers will need to be off-boarded.

A good indicator of the maturity of a SIAM organisation is how smoothly these events can be handled, ideally in a manner which is largely invisible to the business users.

A great deal of thought and planning needs to go into developing processes for on-boarding new suppliers, transitioning work between suppliers, and off-boarding suppliers. Part of this needs to include working with Supplier and Contract Management staff to ensure that contracts consider all parts of the contractual lifecycle, including what needs to happen at contract close, whether this is due to services transitioning to another supplier or simply being decommissioned.

The process is likely to need to be refined over time, with lessons learnt and improvement actions identified.

To help govern this, within the SIAM Governance Framework we have the following components:

- Supplier and Contract Management process
- Supplier On-boarding, Transition and Off-boarding process
- SIAM Governance Board
- Continual Service Improvement
- Risk Management (to identify and manage supplier related risks)

Supplier and Contract Management

Within a SIAM ecosystem, the range of suppliers, potentially each with multiple contracts, and possibly for different layers of different services, needs effective management. Depending on the SIAM model adopted, this management may be happening at multiple levels (within the retained organisation and within the Service Integrator).

At each level, within the relevant scope, operational governance needs to make sure that Supplier and Contract Management is in place and being effective in the following activities:

- Ensuring that suppliers fulfil their contractual obligations
- Ensuring suppliers conform with key organisational policies such as those for security
- Ensuring that any contractual exit obligations are fulfilled
- Ensuring that the responsibilities of the different suppliers are understood by all parties
- Monitoring and reviewing supplier performance
- Ensuring timely availability of inputs to Financial Management regarding service delivered and penalties
- Working with suppliers to agree and implement any corrective actions
- Identifying supplier related risks and corresponding mitigation plans
- Agreeing timely contract changes and renewals/extensions
- Managing contract terminations and scheduled exits

To help govern this, within the SIAM Governance Framework we have the following components:

- Supplier and Contract Management process
- KPIs and metrics
- Service Reporting process
- Supplier On-boarding, Transition and Off-boarding process
- SIAM Governance Board
- Risk Management (to identify and manage supplier related risks)

Monitoring and Review

A set of Key Performance Indicators (KPIs) should be defined for measuring performance within the SIAM ecosystem at different levels. These KPIs should be aligned with relevant business objectives, the SIAM strategy objectives and any contractual measures. Where possible, the KPIs should measure common indicators across different suppliers in the eco-system, to enable comparison and evaluation of service quality. These KPIs should be supplemented by additional metrics that will be used to monitor current activities and workloads, identify trends and backlogs, and understand whether resources need to be redeployed.

Where there is a reliance on supplier provided KPIs and metrics, organisations need to consider applying appropriate controls, especially where they are related to contractual measures which might have significant financial implications. These controls will tend to be related to either the ability of the client organisation to verify the measurement themselves, or the visibility they have with regards to how the supplier figures are measured (including what is deemed in scope), calculated and presented. In the long run, transparency and clarity will benefit both sides as it helps build both trust and a common understanding.

There's no point monitoring and reporting metrics, unless these are actually reviewed, understood and when needed, action taken as a result of them. Reviews should occur regularly and should be focused on a number of areas as described below.

Overall SIAM Performance

Retained IT should be monitoring the performance and throughput of the SIAM ecosystem as a whole, in order to understand:

- Progress towards strategic objectives
- Overall performance in terms of efficiency, effectiveness and quality

- Workload trends, backlogs and achievements
- Areas that require improvement

Integrator Performance

Retained IT should be monitoring and reviewing the performance of the Service Integrator, no matter whether this is performed in-house or is out-sourced. The focus should be on ascertaining how well the role and responsibilities of the Service Integrator are being performed, so it is important to pick KPIs that will be indicative of integrator performance rather than events that are outside their control. As well as providing any contractual measurements the reporting and review of KPIs and metrics should include looking at:

- Understanding any workload trends or variances
- Measurement of efficiency, effectiveness and quality
- Identification of areas for improvement

Supplier Performance

The performance of each supplier should be monitored, and this tends to be done by the organisation to which they are contracted. Reporting and review should include any contractual requirements, but also cover the points above.

In many cases, suppliers will need to interact with each other, and how well this works may set the tone for the SIAM programme. There's sometimes the tendency to assume all parties will be good corporate citizens and play nicely together, but given the reality of competition and commercial pressures, it's worthwhile keeping a close eye on this.

Process and Function Achievements

As with any Service Management implementation, monitoring and review should also occur at both process and function level, to understand workloads, backlogs and performance. It is worthwhile selecting a range of measures including ones that relate to efficiency, effectiveness and quality.

Process Governance

Process governance needs to occur with the Process Owners and Process Managers ensuring that:

- Roles are allocated and agreed, and re-allocated when people leave or move role
- Responsibilities are understood and performed
- Process documentation is maintained and available
- The process is 'policed' and not bypassed
- Process policies are understood and conformed with
- People are aware of the process, including when and how to use it
- Process outputs are of an acceptable quality
- Process integrations are performing as expected
- Related risks are identified and managed
- Appropriate resources and budget are allocated
- Improvements are identified and implemented

Document Governance

As with the strategic SIAM documentation, consideration must be given to governing SIAM operational documentation. This includes documentation for the individual processes and tools deployed, as well as service improvement plans and reports.

Some of these documents (such as policies, processes and procedures) should be subject to change control while others (such as reports and handover notes) may just need appropriate storage, where they can be located and accessed when required.

Operational Review Cycle

Key operational documents such as those covering processes and procedures, should be periodically reviewed (at least annually) to ensure that they are still current and relevant. Each document should have an assigned owner who will be responsible for facilitating the review and ensuring any necessary updates are implemented.

Auditing

Audit is an important governance tool, allowing the strength and effectiveness of controls to be periodically tested, weaknesses identified and improvements made. The Audit process should provide assurance to senior management that the SIAM strategy and model are being properly governed and controlled. The SIAM Governance Board should work with the audit function to put in place appropriate audit policies, plans and schedules, and ensure that issues identified by audits are owned and addressed.

Continual Service Improvement

All of the processes and functions should be subject to Continuous Service Improvement (CSI), with potential improvements identified, agreed and implemented in a controlled manner. Any governance issues, such as the bypassing of processes or poorly maintained documentation, should be rectified as part of these improvements.

6. Summary

Good effective governance is key to successful SIAM, both during implementation and on-going operation. Such implementations are generally complex and are being done against the already complex IT landscape that most organisations now have, so there's no point hoping that the designed SIAM solution will sail gracefully through the many risks without a mechanism there to steer and control it. Organisations need to develop and implement a SIAM Governance Framework that fits their needs and culture, by adopting and adapting the guidance provided within this document.