Service Integration and Management (SIAM®) Foundation Process Guides

Version Date:16th January 2017

SIAM® F Process Guides

License Information Summary

See Appendix A for the detailed license information applying to this document.

You are free to:

- Share — copy and redistribute the material in any medium or format

Under these terms:

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

- Non-commercial — You may not use the material for commercial purposes.

- No Derivatives — If you remix, transform, or build upon the material, you may not distribute the modified material.

- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

SIAM®F Process Guides

Contents

SIAM®F Process Guides

About this Document

Authors and Contributors

Document Purpose

This document describes some of the common processes that support service integration and management (SIAM). It is not an exhaustive list of processes that support SIAM; its contents are part of the source material for the EXIN BCS Service Integration and Management Foundation (SIAM®F) certification.

SIAM®F Process Guides

1.   What is a Process?

A process is *"a documented, repeatable approach to carrying out a series of tasks or activities"*

Most business activities involve repeated tasks; for example, taking a phone call from a customer, raising an invoice, or managing a complaint.

Documenting a process for a repeated task has several benefits:

- It allows the organization to define its preferred approach to managing the task
- The task will be carried out consistently
- It avoids staff wasting time recreating an approach each time the task is carried out
- New staff can be quickly trained to carry out a process
- It can be measured and assessed
- It can be used as a baseline for improvement

A process takes one or more inputs, performs activities on them, and transforms them into one or more outputs.

A process description document will normally include:

- The purpose and objectives of the process
- The trigger for starting the process
- Process activities or steps
- Roles and responsibilities, including a RACI model
- Metrics for the process, including service levels, targets, and key performance indicators
- Process inputs and outputs
- Escalation paths
- Associated toolsets
- Data and information requirements

Every process should have an owner. The owner is the single, accountable role that ensures the process is correctly defined, executed and reviewed. In larger organizations, process manager roles might also be part of the organizational structure; these roles are responsible for the execution of process activities.

For example, the process owner for change management might be the organization's change manager. They could be supported by a number of change analysts, who would be fulfilling process manager-type roles.

Processes are part of an organization's SIAM model.

This document describes some common processes at a high level, and also includes SIAM considerations to help organizations start to adapt processes within a SIAM ecosystem.

This is not an exhaustive list of processes used within SIAM ecosystems; neither is it an in-depth process guide for commonly used service management processes that are fully described in other management practices, frameworks and standards like ISO/IEC 20000.

Page 10 of 79

2.   Processes and the SIAM Ecosystem

SIAM itself is not a process; however, to operate effectively, it relies on a number of processes.

Most management approaches expect processes to be executed within one organization. Within a SIAM ecosystem, processes are likely to be executed:

- Across different organizations in the same SIAM layer
- Across organizations in different SIAM layers

Processes need to be allocated to the appropriate layers in the SIAM model. This allocation may be different for each implementation of SIAM.

Many of the processes used within a SIAM ecosystem are processes familiar from other practices, for example, change management and business relationship management.

Within a SIAM model, these processes require adaptation and augmentation to support integration and coordination between the different parties involved. They also require alignment with other parts of the SIAM model including:

- SIAM practices
- SIAM layers
- Governance model
- Structural elements

The execution of many processes will span multiple layers, and involve multiple parties. For example, the customer organization and the service integrator can both carry out elements of supplier management; the service integrator and service providers will each have responsibilities in the end to end change management process.

Each service provider might carry out individual process steps in a different way, but as part of an overall integrated process model. Process models are therefore important SIAM artefacts; local processes and work instructions are likely to remain within the domain of the individual organization who performs the activities.

SIAM®F Process Guides

Each party in a SIAM ecosystem should adapt and augment their own processes to integrate with the relevant process models, as part of the overall SIAM model.

The detail of the process models, and the allocation of activities to the different layers in the SIAM structure, will vary for each implementation of SIAM. See the SIAM Body of Knowledge, Section 2: SIAM Roadmap for more information on process models and how to design a SIAM model.

Because each SIAM model is different, this document cannot prescribe who will do what for each process. In all SIAM models, it is important to ensure that the roles and responsibilities, interface and dependencies of the customer, service integrator and service providers are mapped, clearly defined, and clearly understood.

2.1. Process Guides

The process guides in this document provide a generic description for each process, plus an illustration of the considerations that should be made when designing and using the process in a SIAM ecosystem.

Each process guide includes:

- Process purpose
- SIAM considerations
- Generic process information:
    - Activities
    - Example roles
    - Example metrics
    - Example inputs and outputs

3. Common SIAM considerations

This section examines the considerations that are common for all processes in a SIAM ecosystem.

3.1. 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

3.2. Who owns the End to End Process?

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

3.3.   Toolset Considerations

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.

3.4.   Data and Information Considerations

3.4.1. 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.

3.4.2. 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.

3.4.3. 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.

3.4.4. 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.

3.4.5. 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.

3.4.6. How will Compliance and Assurance be Managed?

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.

4. Process Guide: Service Portfolio Management

4.1. Process Purpose

The purpose of service portfolio management is to maintain information on all services, to provide the customer organization with a better insight as to ongoing spend, and support business decisions on future investment in products and services.

The process creates a single source of service information, and tracks the status of planned, current and retired services.

4.2. SIAM Considerations

Service portfolio management considerations in a SIAM environment include:

- 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

4.3. Generic Process Information

4.3.1. Activities

Service portfolio management activities can include:

- Creating a service portfolio
- Maintaining a service portfolio
- Reviewing a service portfolio

4.3.2. Example Roles

Service portfolio management roles can include:

- Service portfolio manager

4.3.3. Example Metrics

Service portfolio management metrics can include:

- Number of planned services
- Number of current services
- Number of retired services
- Commercial viability of services
- Number of portfolio opportunities

4.3.4. Inputs and Outputs

Service portfolio management inputs can include:

- Customer strategy and requirements
- Demand management data
- Service portfolio reviews
- Service catalogues
- Service contracts
- New and changed services

Service portfolio management outputs can include:

- Service portfolio
- Service portfolio reports

- Approved services
- Terminated services

5. Process Guide: Monitoring and Measuring

5.1. Process Purpose

The purpose of the monitoring and measuring process includes:

- Responsibility for the monitoring and measurement of systems and service delivery
- Monitoring services against defined thresholds, creating alerts, identifying and predicting service impacting trends and preventing service interruptions
- Measuring service utilization and performance

This process has relationships with other processes including event management and service level management.

5.2. SIAM Considerations

Monitoring and measuring considerations in a SIAM environment include:

- 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

5.3. Generic Process Information

5.3.1. Activities
Monitoring and measuring activities can include:

- Service monitoring
- Threshold detection
- Event creation
- Report creation
- Performance analysis
- Tuning

5.3.2. Roles
Monitoring and measuring roles can include:

- Service level manager
- Capacity manager
- Availability manager
- Event manager
- Performance manager

5.3.3. Example Metrics
Monitoring and measuring metrics can include:

- Incidents related to capacity/availability issues
- Availability of services
- Performance of services
- Reports issued within schedule

5.3.4. Example Inputs and Outputs
Monitoring and measuring inputs can include:

- Contractual service levels
- Service thresholds
- Alerts
- Service provider data
- Reporting requirements, formats and frequencies

Monitoring and measuring outputs can include:

- Measurement reports
- Service measurements
- Service improvement opportunities
- Events
- Forecasts
- Change requests

6. Process Guide: Event Management

6.1. Process Purpose

Event management is the process by which events are identified through the monitoring of technology components, systems and services and, where appropriate, action is taken.

The process seeks to provide early detection and even avoidance of system and service outages, and increase service availability for users. It is closely related to monitoring and measuring, incident management, and availability management.

6.2. SIAM Considerations

Event management considerations in a SIAM environment include:

- 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

6.3. Generic Process Information

6.3.1. Activities

Event management activities can include:

- Record an event (often automatically created by monitoring systems)
- Diagnose and evaluate the event
- Create an associated incident if required, and assign to the incident management process
- Close the event
- Configure and tune event management tools

6.3.2. Example Roles

Event management roles can include:

- Operations team
- Service desk

6.3.3. Example Metrics

Event management metrics can include:

- Number of events, by type
- Accuracy of event information, by type
- Number of incidents avoided
- Number of failures resolved

6.3.4. Example Inputs and Outputs

Event management inputs can include:

- Auto-generated alerts
- User reports of system failures

Event management outputs can include:

- Event data
- Trend reports

- Input into related processes including incident and problem management

7. Process Guide: Incident Management

7.1. Process Purpose

Incident management records and manages service issues (known as incidents) that are interrupting the availability of a service. The process also manages events that are degrading or could degrade service performance.

The process seeks to restore service. This is often within an agreed timescale, dictated by the priority of the incident, based on its impact and how quickly it needs to be resolved.

7.2. SIAM Considerations

Incident management considerations in a SIAM environment include:

- 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

SIAM®F Process Guides

7.3. Generic Process Information

7.3.1. Activities

Incident management activities can include:

- Incident reporting
- Incident detection
- Incident categorisation and prioritization
- Record creation
- Incident investigation
- Incident resolution
- Confirmation of resolution
- Record updated and closed
- Incident trend analysis

7.3.2. Example Roles

Incident management roles can include:

- Incident manager
- Service desk
- Major incident manager
- Technical staff

7.3.3. Example Metrics

Incident management metrics can include:

- Number of incidents (overall, by service, by site etc.)
- Number of incidents resolved at first point of contact
- Incidents that needed to be reopened
- Customer satisfaction with the incident management process
- Incidents that have been incorrectly assigned

7.3.4. Example Inputs and Outputs

Incident management inputs can include:

- Events
- User reports

Incident management outputs can include:

- Incident records
- Resolved incidents
- Incident reports
- Incident metrics

8. Process Guide: Problem Management

8.1. Process Purpose

Problem management is responsible for managing the lifecycle of a problem, which is defined as the unknown underlying cause of an incident. It is also responsible for preventing incidents and problems from occurring or recurring.

The problem management process has both reactive and proactive aspects: the reactive aspect is concerned with solving problems in response to one or more incidents within an agreed timescale and based on the priority of the problem. The proactive aspect is concerned with preventing incidents from occurring in the first place.

8.2. SIAM Considerations

Problem management considerations in a SIAM environment include:

- 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

8.3. Generic Process Information

8.3.1. Activities

Problem management activities can include:

- Review of incident(s) reported or trend analysis of incident records
- Creating problem records
- Categorising and prioritizing problem records
- Identifying and communicating workarounds
- Identifying and addressing the root cause of a problem
- Proactively identifying and addressing potential problems

8.3.2. Example Roles

Problem management roles can include:

- Problem manager
- Technical teams

8.3.3. Example Metrics

Problem management metrics can include:

- Problems recorded per month – proactive and reactive
- Number of in-progress problems
- Number of resolved problems
- Number of recurring incidents while a problem is being investigated

8.3.4. Example Inputs and Outputs

Problem management inputs can include:

- Incident records
- Configuration management information
- Change records
- Workarounds

SIAM®F Process Guides

Problem management outputs can include:

- Problem records
- Problem reviews
- Resolved problems
- Workarounds
- Change requests
- Service improvements
- Knowledge articles
- Reports

9. Process Guide: Change and Release Management

9.1. Process Purpose
Change management enables changes to be made to services with minimal amounts of disruption.

A release is a collection of one or more changes tested and deployed together. Release management ensures that the integrity of the live environment is protected and that the correct changes are deployed.

Together, the processes ensure that consistent methods are used to assess, approve and deploy changes.

9.2. SIAM Considerations
Change and release management considerations in a SIAM environment include:

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

9.3. Generic Process Information

9.3.1. Activities
Change and release management activities can include:

- Analysis of proposed changes
- Approving changes
- Scheduling of changes
- Communication
- Packaging of releases
- Scheduling of releases
- Testing of releases
- Implementation and deployment
- Reviewing successful deployment

9.3.2. Example Roles
Change and release management roles can include:

- Change requestor
- Change manager
- Release manager
- Test manager
- Product owners
- Change advisory board attendees

9.3.3. Example Metrics
Change and release management metrics can include:

- Changes per month
- Successful changes/releases
- Emergency changes
- Failed changes/releases
- Number of incidents caused by changes

9.3.4. Example Inputs and Outputs

Change and release management inputs can include:

- Change policy
- Release policy
- Requests for change
- Incident and problem data related to changes
- Service targets
- Test results
- Configuration information
- Change and release plans

Change and release management outputs can include:

- Approved/rejected changes
- Change schedules
- Change/release communications
- Release plans
- Service availability plans
- Change reviews

10.   Process Guide: Configuration Management

10.1. Process Purpose

The purpose of configuration management is to identify, record, maintain and assure data and information about configuration items (CIs).

A configuration item can be anything used to deliver or support the services, including:

- A service
- Software application or product
- Hardware component
- Documentation

The types of CIs in scope are tailored on a customer by customer basis. There can be many different types of CI.

CI details are often held in one or more configuration management databases (CMDB). Aggregation of multiple CMDBs and other data sources is referred to as a configuration management system (CMS).

Configuration management records and maintains details of the relationships between CIs, and documents how they interact and rely upon each other.

Configuration management has interfaces with other processes, including:

- Incident management, which registers incidents against CIs, and uses CI information to identify existing incidents for the affected CI or recent changes to it that may have cause an incident
- Change management, which registers changes against CIs and uses configuration management data to assess the potential impact of changes
- Problem management, which uses configuration management information to look for incident trends

10.2. SIAM Considerations

Configuration management considerations in a SIAM environment include:

- 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

10.3. Generic Process Information

10.3.1. Activities

Configuration management activities can include:

- Design and implementation of configuration management database(s)
- Gathering data to populate CMDB(s)
- Updating data based on triggers including change management inputs
- Audit of configuration management data
- Documentation and investigation of any data discrepancies
- Providing reports as required

10.3.2. Example Roles

Configuration management roles can include:

- Configuration manager
- Configuration analyst

10.3.3. Example Metrics

Configuration management metrics can include:

- Number of configuration items (CIs), by service provider, type, status etc.
- Number of CI to CI relationships (by service)
- Number of CIs with incomplete or missing information
- CIs that are verified/unverified
- CIs discovered that are not in the CMDB
- CIs in the CMDB that should be seen by automated discovery tools but are not

10.3.4.   Example inputs and outputs

Configuration management inputs can include:

- Data from discovery tools
- Data and information from physical checks
- Incident records
- Change records
- Build information from infrastructure teams
- Application information from development teams

Configuration management outputs can include:

- CMDB records
- Verification schedules
- Verification reports

11.   Process Guide: Service Level Management

11.1. Process Purpose

Service level management (SLM) ensures that service performance meets agreed requirements. These requirements are set out as service level targets in a contract or service agreement.

SLM contributes to, reviews and validates the service level targets against service provider capability and planned service provision.

Following the implementation of services, SLM will continually review, report on, and drive performance against the targets.

11.2. SIAM Considerations

Service level management considerations in a SIAM environment include:

- 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

11.3. Generic process information

11.3.1. Activities

Service level management activities can include:

- Tracking performance against service level targets
- Validating service reports from service providers
- Producing and publishing reports of service achievements against service levels and of trends
- Reviewing performance data to identify improvement opportunities
- Reviewing service level targets for ongoing alignment with business requirements

11.3.2. Example Roles

Service level management roles can include:

- Service level manager
- Reporting analyst

11.3.3. Example Metrics

Service level management metrics can include:

- Customer perception of the services
- Service level achievement against targets

Service level management metrics are often trended on a monthly, quarterly, and annual basis. This can highlight areas for improvement and successes.

11.3.4. Example Inputs and Outputs

Service level management inputs can include:

- Contracts
- Service targets
- Service provider capabilities
- Service performance data
- Customer feedback

Service level management outputs can include:

- Service level reports
- Trend analysis
- Service improvement opportunities

12.   Process Guide: Supplier Management

12.1. Process Purpose

The supplier management process defines the supplier management policy and strategy, establishes a management framework, and identifies and manages service providers, to deliver value for money to the customer.

The process manages supplier performance, in conjunction with service level management and contract management.

12.2. SIAM Considerations

The 'suppliers' in a SIAM ecosystem are referred to as service providers. Supplier management considerations in a SIAM environment include:

- Effective supplier management is critical to the success of any SIAM implementation. Performance issues with one service provider can affect others, as well as the end to end service
- 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

12.3. Generic Process Information

12.3.1. Activities

Supplier management activities can include:

- Plan, produce and implement a supplier management policy and process
- Enforce the policy
- Design and implement a supplier management framework
- Apply remedies for failure to meet service level targets
- Identify and manage non-conformity to the policy and process
- Escalate to contract management as required

12.3.2. Example Roles

Supplier management roles can include:

- Supplier manager
- Account manager
- Procurement manager
- Service provider service manager

12.3.3. Example Metrics

Supplier management metrics can include:

- Number of suppliers managed in accordance with the policy
- Supplier performance aligned to committed performance targets
- Reduction of service failures
- Accuracy of service reporting and conformity to service level agreements

12.3.4. Example Inputs and Outputs

Supplier management inputs can include:

- Business policy requirements
- Contracts
- Audit reports
- Regulatory and industry standards
- Previous breaches and achievements
- Customer and supplier requirements
- Planned changes
- Project plans and risk logs

Supplier management outputs can include:

- Supplier conformance reports
- Planned improvements and remediation activities
- Training needs

13. Process Guide: Contract Management

13.1. Process Purpose

The purpose of contract management is to:

- Evaluate proposals from prospective service providers
- Negotiate and finalise contracts with service providers
- Verify if contractual requirements are being met, and trigger contractual remediation if required
- Assess if contracts are still relevant, and advise on updates or termination if no longer required

13.2. SIAM Considerations

Contract management considerations in a SIAM environment include:

- 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

13.3. Generic Process Information

13.3.1. Activities

Contract management activities can include:

- Negotiate and agree contracts
- Develop and implement sourcing strategies
- Manage contractual changes
- Verify delivery against contractual requirements
- Address contractual non-compliance

13.3.2. Example Roles

Contract management roles can include:

- Contract manager
- Legal advisor

13.3.3. Example Metrics

Contract management metrics can include:

- Contract renewals within schedule
- Service provider performance against contracts
- Contract breaches

13.3.4. Example Inputs and Outputs

Contract management inputs can include:

- New service portfolio entries
- Contract framework
- Contract change notices
- Escalations from supplier management

Contract management outputs can include:

- Service provider addition and removal plans
- Service improvement plans for under-performing service providers
- Contracts

- Warning notices
- Sourcing strategies

14.   Process Guide: Business Relationship Management

14.1. Process Purpose

The business relationship management (BRM) process is responsible for building and maintaining strong relationships between service providers and the consumers of their services.

BRM's role is to understand how business processes are supported by a service provider's services and processes.   BRM is also responsible for ensuring the right messages are received by the right stakeholders at the right time.

BRM's goal is to create convergence between IT services and business needs, acting as a strategic advisor, not a supporting function.

14.2. SIAM Considerations

BRM considerations in a SIAM environment include:

- The retained capabilities within the customer organization are normally responsible for BRM with the service consumers
- The service integrator may have its own BRM function that has a relationship with the customer organization's retained capabilities, but this is normally part of the service integrator's commercial activities and doesn't necessarily form part of the SIAM model
- Service providers may also have BRM functions, which may also be outside the scope of the SIAM model
- A BRM policy should be developed to ensure consistent communication and stakeholder management
- The business areas that consume services must understand that their point of contact for services is via the customer's retained capabilities, and not directly with the service providers

14.3. Generic Process Information

14.3.1. Activities

BRM activities can include:

- Developing and maintaining stakeholder engagement plans
- Developing and maintaining communication plans
- Meeting with the service integrator, service providers and customers
- Establishing and maintaining stakeholder forums
- Executing communication plans
- Reviewing customer satisfaction

14.3.2. Example Roles

BRM roles can include:

- Business relationship managers
- Communication managers
- Service owners
- Service managers
- Stakeholders

14.3.3. Example Metrics

BRM metrics can include:

- Delivery of communication management plan
- Delivery of communication improvement plans
- Number of improvement initiatives
- Number of satisfaction surveys
- Ratings from satisfaction surveys

14.3.4. Example Inputs and Outputs

BRM inputs can include:

- Communication standards, including templates, logos, and style sheets
- Stakeholder map
- Communication plan
- Customer feedback

BRM outputs can include:

- Communication plan
- Business communications
- Minutes of meetings
- Customer satisfaction reports
- Improvement plans

15. Process Guide: Financial Management

15.1. Process Purpose

The purpose of financial management is to oversee the management of the end to end financial function and the activities of collating, investigating, analysing and presenting financial information to the customer.

15.2. SIAM Considerations

Financial management considerations in a SIAM environment include:

- Maintaining commercial confidentiality across the ecosystem
- Being able to compare and contrast financial information from different services providers in a meaningful way
- Understanding the cost of a service provided by multiple service providers, including the cost drivers of different components
- Presenting consolidated financial information to the customer in an understandable format
- Maintaining traceability of financial information across the SIAM ecosystem

15.3. Generic Process Information

15.3.1. Activities

There are 6 main financial management activities:

- Costing
- Budget planning
- Monthly monitoring of spend against budget
- Produce and maintain financial reports and outputs
- Conduct financial impact analysis
- Process invoices

15.3.2. Example Roles

Financial management roles can include:

- Chief financial officer
- Management accountant
- Cost accountant
- Accounts assistant

15.3.3. Example Metrics

Financial management metrics can include:

- Cost of a service
- Profitability of a service
- Comparison between services and service providers
- Spend against budget
- Accuracy of invoices
- Resolution of invoice discrepancies
- Outputs produced on time

15.3.4. Example Inputs and Outputs

Financial management inputs can include:

- Invoices
- Budget plans
- Contractual pricing models
- Purchase orders
- Service costs

Financial management outputs can include:

- Billing plan
- Reports
- Cost breakdown
- Spend and forecast data
- Financial risk and opportunity information
- Invoices

16.   Process Guide: Information Security Management

16.1. Process Purpose

Information security management (ISM) sets and monitors adherence to security policies and processes. It manages the confidentiality, integrity, and availability of information, data, IT and people.

Its objective is to protect individuals, technology, and organizations from damage caused by system outages, breaches of privacy, malicious attacks, and loss or disclosure of protected data and information.

16.2. SIAM Considerations

Information security management considerations in a SIAM environment include:

- Defining who is accountable for establishing and managing the end to end information security process and policies
- Using consistent information security classifications and definitions. For example, what constitutes a security incident?
- Managing and communicating breaches and identified vulnerabilities across the ecosystem
- Defining responsibility for managing the investigation and resolution of security breaches involving multiple parties
- Including security targets within service provider contracts, for example, giving the authority to suspend a service provider's service if it is compromising other services
- Being aware of increased security risks when lower level risks are aggregated across multiple parties

16.3. Generic Process Information

16.3.1. Activities

Information security management activities can include:

- Plan, produce and implement an ISM policy and process
- Enforce the policy and monitor adherence
- Implement a security toolset
- Monitor security activity and take appropriate resolution or improvement actions
- Identify risks derived from aggregation of lower level risks
- Raise incidents for breaches and failures using the incident management process and service desk
- Evaluate and update the policy, process and tools to ensure protection is maintained
- Plan and deliver training, audits, reviews and tests of the security framework

16.3.2. Example Roles

Information security management roles can include:

- Senior information risk officer
- Information security manager
- Service desk
- Incident manager

16.3.3. Example Metrics

Information security management metrics can include:

- Number of security-related incidents
- Number of security breaches
- Percentage of users complying with security training and other requirements
- Availability and accuracy of security tools and systems
- Accuracy and outcomes of security audits and tests
- Percentage awareness of security principles throughout the organization

16.3.4. Example Inputs and Outputs

Information security management inputs can include:

- Policy requirements
- Regulatory and industry standards
- Previous breach and 'near miss' information
- Planned changes
- Customer and service provider requirements
- Project plans
- Risk logs

Information security management outputs can include:

- Security incident records
- Planned improvements
- Remediation activities
- Training needs
- Disciplinary and human resources action
- Process and policy status reports

17.   Process Guide: Continual Service Improvement

17.1. Process Purpose

The purpose of continual service improvement is to provide a consistent method of quantifying, tracking and managing the delivery of improvement activity across an ecosystem.

Improvement activities can be applied to people, processes, services, technology, and the interfaces and relationships between them.

17.2. SIAM Considerations

Continual service improvement considerations in a SIAM environment include:

- There should be a common definition of continual service improvement across all parties in the ecosystem
- Continual service improvement should be on the agenda of governance boards
- Continual service improvement should be the primary focus of the process forum structural elements
- All service providers should be encouraged and incentivised to contribute to continual service improvement activities
- There should be an approach to share lessons learned across all parties in the SIAM ecosystem
- There may be a need to a central database or register of continual service improvement activities
- The service integrator will be responsible for managing cross-service provider improvements
- There needs to be a mechanism in place to prioritize improvements to the end to end services and processes

17.3. Generic Process Information

17.3.1. Activities

Continual service improvement activities can include:

- Investigation: the improvement is identified and further information obtained
- Baseline: document current metrics
- Identify and quantify the expected or desired improvements and benefits
- Categorize and prioritize the improvement, to define the required level of governance and relative importance
- Approve further activity
- Stakeholder management and communication planning
- Plan improvement
- Carry out improvement actions
- Review improvement
- Measure, review, and quantify benefit
- Close improvement action, including documenting lessons learned

17.3.2. Example Roles

Continual service improvement roles can include:

- Improvement initiator
- Improvement sponsor
- Improvement implementer
- Governance board attendees
- Process forum attendees

17.3.3. Example Metrics

Continual service improvement metrics can include:

- Number of improvements identified, active, and completed
- Cost of improvement activities
- Increased value associated with improvement activities
- Improvements in achievement of service level targets and process performance indicators

17.3.4. Example Inputs and Outputs

Continual service improvement inputs can include:

- Management information including service level reports, internal key performance indicator reporting, trend analysis
- Lessons learned reviews
- Audits
- Customer satisfaction reports
- Strategic drivers including delivery model evaluation, industry bench marking, governance board outputs

18.   Process Guide: Knowledge Management

18.1. Process Purpose

Knowledge Management is the process of capturing knowledge and making it available in a controlled and quality-assured manner to all appropriate people.

18.2. SIAM Considerations

Knowledge management considerations in a SIAM environment include:

- Standardised templates and definitions for knowledge can be useful to ensure consistent capture and dissemination
- Service providers should be encouraged to share knowledge with each other
- Responsibilities for creating, reviewing, approving, publishing, and maintaining knowledge articles must be clearly defined
- Relevant parties must be able to access knowledge, either from a single knowledge repository, or a virtual repository linking all providers
- Knowledge should be consistent across the SIAM ecosystem

18.3. Generic Process Information

18.3.1. Activities

Knowledge management activities can include:

- Knowledge identification, capture and maintenance
- Knowledge transfer
- Data and information management
- Evaluation and improvement

18.3.2. Example Roles

Knowledge management roles can include:

- Knowledge creator
- Knowledge manager
- Knowledge editor

18.3.3. Example Metrics

Knowledge management metrics can include:

- Number of knowledge users
- Reduction in incident resolution time owing to use of knowledge items
- Percentage of incidents resolved by referral to knowledge items
- Number of active knowledge articles
- Frequency of updates
- Frequency of access by article
- Accuracy of repository content
- Reduction in time spent on knowledge rediscovery

18.3.4. Example Inputs and Outputs

Knowledge management inputs can include:

- Documented observations
- External knowledge sources
- Data and process information
- Data repositories
- Release notes
- Procedures manuals

- Training material

Knowledge management outputs can include:

- Knowledge articles
- Reports
- Updated knowledge management system
- Archived data and information
- Updated training materials

19. Process Guide: Toolset and Information Management

19.1. Process Purpose

The purpose of toolset and information management is to provide toolset(s) to support the other processes, facilitate information sharing, and manage data, information, and knowledge.

19.2. SIAM Considerations

In SIAM models, there may be a single toolset, or many toolsets. Toolset and information management considerations in a SIAM environment include:

- Defining and managing the use of consistent standards for data, information, and knowledge across all service providers
- Creating the toolset strategy for the SIAM model
- Creating an enterprise toolset architecture for the SIAM ecosystem
- Selecting an appropriate toolset in line with the strategy and enterprise architecture
- Defining, implementing, and maintaining integration between the toolsets of different parties

19.3. Generic Process Information

19.3.1. Activities
Toolset and information management activities can include:

- Toolset selection
- Toolset implementation
- Toolset management and maintenance
- Data and information standards definition
- Toolset integration

19.3.2. Example Roles
Toolset and information management roles can include:

- Toolset architect
- Toolset developer
- Toolset manager
- Data and information architect
- Data and information manager
- Toolset service provider

19.3.3. Example Metrics
Toolset and information management metrics can include:

- Toolset availability
- Toolset reliability
- Toolset data quality

19.3.4. Example Inputs and Outputs
Toolset and information management inputs can include:

- Configuration data
- Interface schema and designs
- User data
- Data repositories

Toolset and information management outputs can include:

- Toolset
- Performance reports
- Service level reports
- Data and information standards
- Data dictionary
- Data interchange standards
- Information classification

20.   Process Guide: Project Management

20.1. Process Purpose

The purpose of project management is to provide a structured approach that delivers projects on time, on budget and at the appropriate level of quality.

20.2. SIAM Considerations

Project management in a SIAM environment manages the end to end outcomes of projects across multiple service providers.

Considerations include:

- The increased complexity of project relationships within a SIAM ecosystem
- Accounting for the fact that there is no direct contractual relationships the service integrator and service providers
- Planning integrated projects involving multiple project teams in multiple service providers
- Obtaining consistency in reporting project status and progress
- Establishment of a collaborative culture to support cross-service provider project management
- Managing risks in integrated projects
- Ensuring effective acceptance into service criteria for project implementations across multiple service providers

20.3. Generic Process Information

20.3.1. Activities

Project management activities can include:

- Planning
- Adhering to organizational policies and requirements
- Directing actions
- Status reporting
- Risk and issue management
- Delivery of change requests
- Quality management of deliverables
- Managing stakeholders

20.3.2. Example Roles

Project management roles can include:

- Project director
- Project manager
- Project management office

20.3.3. Example Metrics

Project management metrics can include:

- Delivery against plan
- Delivery against quality requirements
- Delivery against budget
- Overdue products
- Customer satisfaction

20.3.4. Example Inputs and Outputs

Project management inputs can include:

- Proposals
- Purchase orders
- Project plans
- Project change requests

- Customer requirements
- Quality criteria

Project management outputs can include:

- Completed projects
- Delivered products
- Plans
- Tasks
- Lessons learned

21.   Process Guide: Audit and Control

21.1. Process Purpose

The purpose of audit and control is to provide assurance that the services provided to the customer are being delivered in accordance with documented requirements. This can include contracted, legislative, regulatory, and security requirements.

21.2. SIAM Considerations

Audit and control considerations in a SIAM environment include:

- It is desirable to apply the same governance framework across all parties, however this may not be possible for certain service providers, for example commodity cloud service providers
- Each organization should own its risks, however the overall accountability for who will ensure that these have been addressed needs to be clearly defined
- The roles of the customer and service integrator in ensuring security assurance and compliance need to be clearly defined
- Requirements need to be in a format that can be understood by auditors, and must be clear enough to verify if they are being met
- Audits will need to take place across the whole SIAM ecosystem
- Audits should be conducted on integrated processes involving several service providers, as well as on individual service provider processes
- The rights of the service integrator (or another organization) to carry out audits should be included in contracts with service providers

21.3. Generic Process Information

21.3.1. Activities

Audit and control activities can include:

- Auditing an organization's processes and systems
- Quality assurance planning
- Auditing projects
- Identifying non-conformance against requirements
- Recording, presenting, and managing audit findings
- Tracking non-conformances through to closure

21.3.2. Example Roles

Audit and control roles can include:

- Quality manager
- Chief security officer
- Auditor
- Process owner

21.3.3. Example Metrics

Audit and control metrics can include:

- Compliance against requirements
- Number of non-conformances identified, opened, and closed

21.3.4. Example Inputs and Outputs

Audit and control inputs can include:

- Audit scope
- Requirements
- Policies
- Standards
- Processes
- Data and information records
- Performance reports
- Process metrics

SIAM®F Process Guides

Audit and control outputs consist of audit reports, including:

- Audit scope
- Non-conformances
- Evidence
- Observations
- Risks and issues
- Improvement opportunities

Appendix B: License Information

Creative Commons Attribution-Non-commercial-No Derivatives 4.0 International Public License

By exercising the Licensed Rights (defined below), You accept and agree to be bound by the terms and conditions of this Creative Commons Attribution-Non-commercial-No Derivatives 4.0 International Public License ("Public License"). To the extent this Public License may be interpreted as a contract, You are granted the Licensed Rights in consideration of Your acceptance of these terms and conditions, and the Licensor grants You such rights in consideration of benefits the Licensor receives from making the Licensed Material available under these terms and conditions.

Section 1 – Definitions.

a. **Adapted Material** means material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.

b. **Copyright and Similar Rights** means copyright and/or similar rights closely related to copyright including, without limitation, performance, broadcast, sound recording, and Sui Generis Database Rights, without regard to how the rights are labelled or categorized. For purposes of this Public License, the rights specified in Section 2(b)(1)-(2) are not Copyright and Similar Rights.

c. **Effective Technological Measures** means those measures that, in the absence of proper authority, may not be circumvented under laws fulfilling obligations under Article 11 of the WIPO Copyright Treaty adopted on December 20, 1996, and/or similar international agreements.

d. **Exceptions and Limitations** means fair use, fair dealing, and/or any other exception or limitation to Copyright and Similar Rights that applies to Your use of the Licensed Material.

e. **Licensed Material** means the artistic or literary work, database, or other material to which the Licensor applied this Public License.

f. **Licensed Rights** means the rights granted to You subject to the terms and conditions of this Public License, which are limited to all Copyright and Similar Rights that apply to Your use of the Licensed Material and that the Licensor has authority to license.

g. **Licensor** means the individual(s) or entity(ies) granting rights under this Public License.

h. **Non-commercial** means not primarily intended for or directed towards commercial advantage or monetary compensation. For purposes of this Public License, the exchange of the Licensed Material for other material subject to Copyright and Similar Rights by digital file-sharing or similar means is Non-commercial provided there is no payment of monetary compensation in connection with the exchange.

i. **Share** means to provide material to the public by any means or process that requires permission under the Licensed Rights, such as reproduction, public display, public performance, distribution, dissemination, communication, or importation, and to make material available to the public including in ways that members of the public may access the material from a place and at a time individually chosen by them.

j. **Sui Generis Database Rights** means rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended and/or succeeded, as well as other essentially equivalent rights anywhere in the world.

k. **You** means the individual or entity exercising the Licensed Rights under this Public License. **Your** has a corresponding meaning.

Section 2 – Scope.

a. **License grant**.

1. Subject to the terms and conditions of this Public License, the Licensor hereby grants You a worldwide, royalty-free, non-sub licensable, non-exclusive, irrevocable license to exercise the Licensed Rights in the Licensed Material to:

   A. reproduce and Share the Licensed Material, in whole or in part, for Non-commercial purposes only; and

   B. produce and reproduce, but not Share, Adapted Material for Non-commercial purposes only.

2. Exceptions and Limitations. For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.

3. Term. The term of this Public License is specified in Section 6(a).

4. Media and formats; technical modifications allowed. The Licensor authorizes You to exercise the Licensed Rights in all media and formats whether now known or hereafter created, and to make

technical modifications necessary to do so. The Licensor waives and/or agrees not to assert any right or authority to forbid You from making technical modifications necessary to exercise the Licensed Rights, including technical modifications necessary to circumvent Effective Technological Measures. For purposes of this Public License, simply making modifications authorized by this Section 2(a)(4) never produces Adapted Material.

5. Downstream recipients.

    A. Offer from the Licensor – Licensed Material. Every recipient of the Licensed Material automatically receives an offer from the Licensor to exercise the Licensed Rights under the terms and conditions of this Public License.

    B. No downstream restrictions. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, the Licensed Material if doing so restricts exercise of the Licensed Rights by any recipient of the Licensed Material.

6. No endorsement. Nothing in this Public License constitutes or may be construed as permission to assert or imply that You are, or that Your use of the Licensed Material is, connected with, or sponsored, endorsed, or granted official status by, the Licensor or others designated to receive attribution as provided in Section 3(a)(1)(A)(i).

b. **Other rights**.
    1. Moral rights, such as the right of integrity, are not licensed under this Public License, nor are publicity, privacy, and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or agrees not to assert any such rights held by the Licensor to the limited extent necessary to allow You to exercise the Licensed Rights, but not otherwise.

    2. Patent and trademark rights are not licensed under this Public License.

    3. To the extent possible, the Licensor waives any right to collect royalties from You for the exercise of the Licensed Rights, whether directly or through a collecting society under any voluntary or waivable statutory or compulsory licensing scheme. In all other cases the Licensor expressly reserves any right to collect such royalties, including when the Licensed Material is used other than for Non-commercial purposes.

Section 3 – License Conditions.

Your exercise of the Licensed Rights is expressly made subject to the following conditions.

a. **Attribution**.
1. If You Share the Licensed Material, You must:
    A. retain the following if it is supplied by the Licensor with the Licensed Material:

    i. identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);

    ii. a copyright notice;

    iii. a notice that refers to this Public License;

    iv. a notice that refers to the disclaimer of warranties;

    v. a URI or hyperlink to the Licensed Material to the extent reasonably practicable;

    B. indicate if You modified the Licensed Material and retain an indication of any previous modifications; and

    C. indicate the Licensed Material is licensed under this Public License, and include the text of, or the URI or hyperlink to, this Public License.

    For the avoidance of doubt, You do not have permission under this Public License to Share Adapted Material.

2. You may satisfy the conditions in Section 3(a)(1) in any reasonable manner based on the medium, means, and context in which You Share the Licensed Material. For example, it may be reasonable to satisfy the conditions by providing a URI or hyperlink to a resource that includes the required information.

3. If requested by the Licensor, You must remove any of the information required by Section 3(a)(1)(A) to the extent reasonably practicable.

Section 4 – Sui Generis Database Rights.

Where the Licensed Rights include Sui Generis Database Rights that apply to Your use of the Licensed Material:

a. for the avoidance of doubt, Section 2(a)(1) grants You the right to extract, reuse, reproduce, and Share all or a substantial portion of the contents of

the database for Non-commercial purposes only and provided You do not Share Adapted Material;

b. if You include all or a substantial portion of the database contents in a database in which You have Sui Generis Database Rights, then the database in which You have Sui Generis Database Rights (but not its individual contents) is Adapted Material; and

c. You must comply with the conditions in Section 3(a) if You Share all or a substantial portion of the contents of the database.

For the avoidance of doubt, this Section 4 supplements and does not replace Your obligations under this Public License where the Licensed Rights include other Copyright and Similar Rights.

Section 5 – Disclaimer of Warranties and Limitation of Liability.

a. **Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to You.**

b. **To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to You.**

c. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

Section 6 – Term and Termination.

a. This Public License applies for the term of the Copyright and Similar Rights licensed here. However, if You fail to comply with this Public License, then Your rights under this Public License terminate automatically.

b. Where Your right to use the Licensed Material has terminated under Section 6(a), it reinstates:

1. automatically as of the date the violation is cured, provided it is cured within 30 days of Your discovery of the violation; or

2. upon express reinstatement by the Licensor.

For the avoidance of doubt, this Section 6(b) does not affect any right the Licensor may have to seek remedies for Your violations of this Public License.

c. For the avoidance of doubt, the Licensor may also offer the Licensed Material under separate terms or conditions or stop distributing the Licensed Material at any time; however, doing so will not terminate this Public License.

d. Sections 1, 5, 6, 7, and 8 survive termination of this Public License.

Section 7 – Other Terms and Conditions.

a. The Licensor shall not be bound by any additional or different terms or conditions communicated by You unless expressly agreed.

b. Any arrangements, understandings, or agreements regarding the Licensed Material not stated herein are separate from and independent of the terms and conditions of this Public License.

Section 8 – Interpretation.

a. For the avoidance of doubt, this Public License does not, and shall not be interpreted to, reduce, limit, restrict, or impose conditions on any use of the Licensed Material that could lawfully be made without permission under this Public License.

b. To the extent possible, if any provision of this Public License is deemed unenforceable, it shall be automatically reformed to the minimum extent necessary to make it enforceable. If the provision cannot be reformed, it shall be severed from this Public License without affecting the enforceability of the remaining terms and conditions.

c. No term or condition of this Public License will be waived and no failure to comply consented to unless expressly agreed to by the Licensor.

d. Nothing in this Public License constitutes or may be interpreted as a limitation upon, or waiver of, any privileges and immunities that apply to the Licensor or You, including from the legal processes of any jurisdiction or authority.