Cloud security governance framework



Table of contents

[Executive Summary 4](#_Toc157512512)

[Terms and abbreviations 5](#_Toc157512513)

[1 Introduction 5](#_Toc157512514)

[2 Direct 5](#_Toc157512515)

[2.1 Tasks 5](#_Toc157512516)

[2.2 Responsibe parties 6](#_Toc157512517)

[2.3 Direct Process RACI Matrix 6](#_Toc157512518)

[3 Monitor 7](#_Toc157512519)

[3.1 Tasks 7](#_Toc157512520)

[3.2 Responsible Parties 7](#_Toc157512521)

[3.3 Monitor Process RACI Matrix 7](#_Toc157512522)

[4 Evaluate 8](#_Toc157512523)

[4.1 Tasks 8](#_Toc157512524)

[4.2 Responsible Parties: 8](#_Toc157512525)

[4.3 Evaluate Process RACI Matrix 8](#_Toc157512526)

[References 9](#_Toc157512527)

| Version | Date | Change comments | Author | Approved |
| --- | --- | --- | --- | --- |
| 0.1 | 01.01.2021 | First edition | Lead architect | CEO |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Executive Summary

**Overview**

The Cloud Security Governance Framework is designed to manage and mitigate security risks in a complex multi-cloud environment. It outlines a structured approach centered around three core processes: Direct, Monitor, and Evaluate. These processes ensure that security governance is comprehensive, proactive, and adaptable to the evolving cloud landscape.

**1. Direct**

The Direct process involves establishing the strategic direction for cloud security, including policy development, defining roles, and ensuring compliance. The RACI matrix for this process highlights the Cloud Security Governance Committee (CSGC) and the Chief Information Security Officer (CISO) as key accountable and responsible parties, respectively. It emphasizes collaboration and consultation with Cloud Security Architects, Compliance Officers, IT Departments, and Business Units to align security governance with business objectives and regulatory requirements.

**2. Monitor**

This process focuses on the continuous oversight of security controls, incident detection, compliance monitoring, and performance reporting. The Cloud Security Operations Team plays a pivotal role, being primarily responsible for the execution of monitoring tasks. The matrix also identifies the CSGC as accountable for overseeing this process, with significant involvement from Internal Audit Teams, IT Departments, and Cloud Service Providers (CSPs) to ensure comprehensive monitoring and compliance.

**3. Evaluate**

The Evaluate process assesses the effectiveness of the security governance framework, identifies improvement areas, and adapts to new risks and technologies. The CSGC, along with the CISO, are central to this process, ensuring that the framework remains effective and aligned with organizational goals. The Risk Management Team, Cloud Security Operations Team, IT Department, Business Units, and CSPs are engaged in various capacities to provide feedback, assess risks, and implement improvements.

**Conclusion**

The Cloud Security Governance Framework provides a clear and actionable roadmap for organizations to secure their multi-cloud environments effectively. Through the structured Direct, Monitor, and Evaluate processes and the delineation of roles and responsibilities via RACI matrices, the framework ensures that all stakeholders are engaged and accountable, thereby enhancing the organization's security posture in a multi-cloud context. This executive summary encapsulates the essence of the framework and the strategic approach to cloud security governance, offering leaders a concise guide to implementing robust multi-cloud security governance practices.

## Terms and abbreviations

|  |  |
| --- | --- |
| **Term** | **Description** |
| CSGC | Cloud Security Governance Committee |
| CISO | Chief Information Security Officer |
| CSP | Cloud Service Providers |
| SOC | Security Operations Center |
| KPI | Key Performance Indicators |

# Introduction

In an era where cloud computing is pervasive, organizations often leverage multiple cloud platforms to fulfill their diverse needs. This multi-cloud environment, while offering scalability, flexibility, and redundancy, introduces complex security challenges. The Cloud Security Governance Framework outlined herein is designed to establish robust governance over such environments. It is structured around three core processes: Direct, Monitor, and Evaluate. This document delineates the tasks associated with each process and identifies the responsible parties.

## The Cloud Security Governance process

The cloudsarc methodology is the foundation for a simple and practical approach to cloud security governance.

The input to the cloud security governance process are the outputs from previous stages in the methodology. We leverage the Security & compliance specification, the cloud security strategy and the risk assessment as inputs to the cloud security governance process. The cloudsarc cloud security governance framework will be implemented using the operational stages of the cloudsarc methodology.

The cloudsarc cloud security governance framework implements three main processes:

**Direct** where Security Governance can establish policies and define a pack of metrics to be measured in an interactive and step by step way.

**Monitor** where measurements are gathered during the processes are enacted. Monitoring requires to include pieces of software at the processes that enable to collect information about the metrics.

**Evaluate** enables the Security Governance to analyse the different metrics in order to decide whether new countermeasures should be applied. This process can be carried out manually when governance needs or a report can be obtained regularly.



Figure 1 Cloud security governance process

# Direct

The Direct process establishes the strategic direction for security governance across all cloud environments. It involves setting policies, defining roles and responsibilities, and ensuring alignment with the organization's overall security strategy.

## Tasks

1. Policy Development and Standardization:
* Develop comprehensive security policies that address specific risks in a multi-cloud environment.
* Standardize security policies across all cloud platforms to ensure consistent application.
1. Roles and Responsibilities Definition:
* Define clear roles and responsibilities for all stakeholders involved in cloud security governance.
* Establish a Cloud Security Governance Committee (CSGC) to oversee policy implementation and compliance.
1. Alignment with Business Objectives:
* Ensure that security governance policies and practices align with the organization's overall business objectives and risk appetite.
1. Compliance and Regulatory Alignment:
* Align security policies with relevant legal, regulatory, and compliance requirements.

## Responsibe parties

* Cloud Security Governance Committee (CSGC)
* Chief Information Security Officer (CISO)
* Cloud Security Architects
* Compliance Officers

## Direct Process RACI Matrix

| **Task** | **CSGC** | **CISO** | **Cloud Security Architects** | **Compliance Officers** | **IT Department** | **Business Units** |
| --- | --- | --- | --- | --- | --- | --- |
| Policy Development and Standardization | A | R | C | C | I | I |
| Roles and Responsibilities Definition | A | R/I | R | I | C | C |
| Alignment with Business Objectives | C | A | I | I | R | R |
| Compliance and Regulatory Alignment | C | R | I | A | I | I |

**A (Accountable):** The party ultimately answerable for the correct and thorough completion of the deliverable or task.

**R (Responsible):** The party responsible for the execution of the task.

**C (Consulted):** Those whose opinions are sought; two-way communication.

**I (Informed):** Those who are kept up-to-date on progress; one-way communication.

# Monitor

The Monitor process involves continuous oversight of security controls, activities, and compliance status across all cloud platforms.

## Tasks

1. Continuous Monitoring:
* Implement tools and practices for continuous monitoring of security controls and configurations across all cloud environments.
* Monitor for unusual activities that may indicate security incidents or policy violations.
1. Security Incident Detection:
* Deploy advanced threat detection tools and services to identify potential security incidents promptly.
1. Compliance Monitoring:
* Regularly review and audit cloud environments to ensure compliance with internal policies and external regulations.
1. Performance Metrics and Reporting:
* Develop and maintain a set of key performance indicators (KPIs) to measure the effectiveness of security controls.
* Regularly report the security status to the CSGC and other relevant stakeholders.

## Responsible Parties

* Security Operations Center (SOC)
* Cloud Service Providers (CSPs)
* Internal Audit Team
* CSGC

## Monitor Process RACI Matrix

| **Task** | **SOC** | **CSPs** | **Internal Audit Team** | **CSGC** | **CISO** | **IT Department** |
| --- | --- | --- | --- | --- | --- | --- |
| Continuous Monitoring | R | C | I | A | I | C |
| Security Incident Detection | R | C | I | I | A | I |
| Compliance Monitoring | C | I | R | A | I | I |
| Performance Metrics and Reporting | R | I | C | A | I | C |

# Evaluate

The Evaluate process involves assessing the effectiveness of the governance framework, identifying areas for improvement, and adapting to evolving security landscapes.

## Tasks

1. Framework Effectiveness Assessment:
* Conduct regular assessments to evaluate the effectiveness of the security governance framework.
* Utilize feedback from audits, incidents, and monitoring reports to assess the performance of security controls.
1. Risk Assessment and Management:
* Regularly perform risk assessments to identify and evaluate new risks in the multi-cloud environment.
* Update risk management strategies and security controls in response to identified risks.
1. Adaptation and Continuous Improvement:
* Continuously update and improve the security governance framework based on assessment findings, technological advancements, and evolving threat landscapes.
1. Stakeholder Feedback and Engagement:
* Engage with key stakeholders, including business units, IT teams, and CSPs, to gather feedback and ensure the security governance framework meets the organization's needs.

## Responsible Parties:

* CSGC
* CISO
* Risk Management Team
* All Cloud Security Stakeholders

## Evaluate Process RACI Matrix

| **Task** | **CSGC** | **CISO** | **Risk Management Team** | **SOC** | **IT Department** | **Business Units** | **CSPs** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Framework Effectiveness Assessment | A | R | C | C | I | I | I |
| Risk Assessment and Management | C | A | R | I | C | C | I |
| Adaptation and Continuous Improvement | A | R | C | C | C | C | C |
| Stakeholder Feedback and Engagement | A | R | I | I | R | R | C |