Domain 2: Cloud Governance and Strategies

This domain focuses on cloud governance with an emphasis on the role of security. Enterprise governance plays a key role in an organization's success and helps in aligning the strategic, tactical, and operational capabilities of information and technology with the business objectives.

ISACA[8] defines *governance* as: "Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives."

As information technology (IT) is moving from supporting back-office functions to becoming front and center of most organizations' strategy and operations, a comprehensive perspective on all stakeholder needs is required. This requires that IT and cloud decisions are embedded in the organization's governance.

Learning Objectives

In this domain, you will learn to:

- Identify the purpose of cloud governance.
- Define the governance hierarchy in cloud governance.
- Explore key strategies and concepts affecting governance in cloud computing.

2.1. Cloud Governance

Cloud computing's multi-tenancy, shared responsibility, distributed supply chains, legal and regulatory complexity, and security concerns require effective governance. Cost efficiency and speed to market are key drivers for cloud adoption. Organizations save costs by moving from Capital Expenditure (CapEx, or investments) to Operational Expense (OpEx, subscription) models, often using *lift and shift* strategies, which require strong security governance to manage new risks from more complex cloud architectures and shared service models.

[8] ISACA. (2024) Glossary - *Governance*

Strategic innovation drives cloud adoption as it enables rapid software development and deployment. However, accelerated deployment cycles introduce governance risks, such as misconfigurations, software supply chain issues, and potential compliance changes. Governance is required to balance between the requirement for speed and the need to control risks.

There are two primary ways cloud affects security governance:

1. The introduction of the Shared Responsibilities Model. Security governance responsibilities are now shared between the cloud provider and the cloud customer. To complicate matters, third-party service providers are sometimes introduced into the security responsibility supply chain. Even if some of the responsibilities are offloaded to a third party, the accountability of the control remains with the cloud service provider (CSP) or cloud service customer (CSC). Compliance risk is always with the CSC.

2. The technical and operational differences are created by the inherent nature of cloud computing. This includes multi-tenancy, geography of data, and platform failover to other regions.

Here are some of the complexities that effective cloud governance has to address:

- Cloud might impose a loss of direct control over the IT infrastructure, forcing an organization to adopt a new governance framework and process.
- Cloud services and data may span multiple jurisdictions, forcing customers to comply with more laws and regulations, especially privacy requirements.
- Visibility and transparency in some cloud services can be challenging.
- Using cloud solutions does not mean outsourcing the organizational accountability of its controls to a third or fourth party.
- Data ownership rights and classification as well as privacy control might not be intuitively clear and need careful examination.
- Most providers have a standard offering that cannot be customized according to all customer's specific requirements.
- Cloud providers might demonstrate different levels of maturity and a variety of services, licenses, and models, which complicates the adoption of a one-size-fits-all cloud policy.
- Cloud services are often built on a chain of providers, which makes scoping governance activities challenging (e.g., a SaaS provider that is running on the infrastructure of an IaaS provider).
- Cloud services employ various shared responsibility models, which differ based on the provider and the technology stack. This necessitates a clear delineation of controls and responsibilities between the cloud service provider and the customer. Adding to the complexity of cloud governance, the shared responsibility model often involves multiple parties. These parties may include cloud platform integrators or brokers, software development companies for applications running on cloud services, different Development and Operations (DevOps) teams, and other stakeholders.
- Hybrid cloud models can complicate governance due to the complexities of producing clear boundaries between provider responsibilities and customer responsibilities.
- Cloud customers have to rely more on compliance and assessment activities rather than actual testing. This will depend on what layers fall into the customer's responsibility. The customer is still responsible for security testing applications in an IaaS model for example. Primarily the customers would have to rely on third-party security assessment reports and certifications of the CSP and

understand the shared responsibilities that the customer has to abide by for the total compliance coverage.
- CPSs may change rapidly, which has to be accounted for in governance models.
- Utilization of cloud services may require additional skills that may or may not currently be present in the organization, such as cloud auditing skills or cloud security skills, as well as knowledge of cloud-oriented security tools.

Effective cloud governance requires the implementation of a strong framework and policies for secure, compliant, and efficient management of cloud resources. Cloud governance includes:

- Defining roles and responsibilities
- Conducting requirements and information gathering
- Managing risks
- Classifying data and assets
- Complying with legal and regulatory requirements
- Maintaining a cloud registry
- Establishing a governance hierarchy
- Leveraging cloud-specific security frameworks

The rest of this Study Guide introduces these topics in more detail and also gives insight into some developments that challenge historical assumptions on IT governance.

- DevOps and Development, Security, and Operations (DevSecOps) (see Domain 10) drive the automation of security controls, which changes organizational structures.
- Zero Trust (ZT) (see Domain 12) drives a fundamentally more comprehensive approach to things like network security, which requires policies to be defined on a different level.
- Artificial Intelligence (AI) and Machine Learning (ML) (Domain 12 and others) open up entirely new fields of applications for which there are few existing governance practices.

2.2 The Governance Hierarchy

A key aspect of cloud governance is establishing a governance hierarchy and defining decision-making processes and escalation paths. This ensures appropriate decision levels and clear accountability.

It's important to use one or more Frameworks to set a road map for your program and security controls. This makes it easier to show compliance. At the top of the hierarchy is a Risk Framework, providing guidelines for evaluating cybersecurity risks. Examples include NIST 800-30, ISO 27005, CIS RAM, and FAIR. Next is the Program framework, which defines the components of your security program; examples include NIST Cybersecurity Framework (CSF), ISO 27001, or Control Objectives for Information and Related Technology (COBIT), and then there are Control Frameworks, which provide a list of technical and procedural controls to apply to the infrastructure; these include NIST 800-53, Center for Internet Security Critical Security Controls (CIS CSC), and Cloud Security Alliance Cloud Controls Matrix (CSA CCM).

The output of these frameworks are tiers of governance documents that define specific structures and actions for your organization. These include:

- Policies outline an organization's security requirements, translating framework guidelines into actionable statements. They ensure adherence to regulatory and compliance requirements.
- Control Objectives, or Guidelines, more specific than policies, focus on desired security control outcomes to minimize risk and maintain a secure environment, for example, requiring MFA for all cloud platform logins. They provide clear security goals for organizations.
- Control Specifications and Technical Standards or Guidance are technical implementations to meet control objectives. For example, a specification might require enabling MFA for user access and applying a technical policy to enforce it.

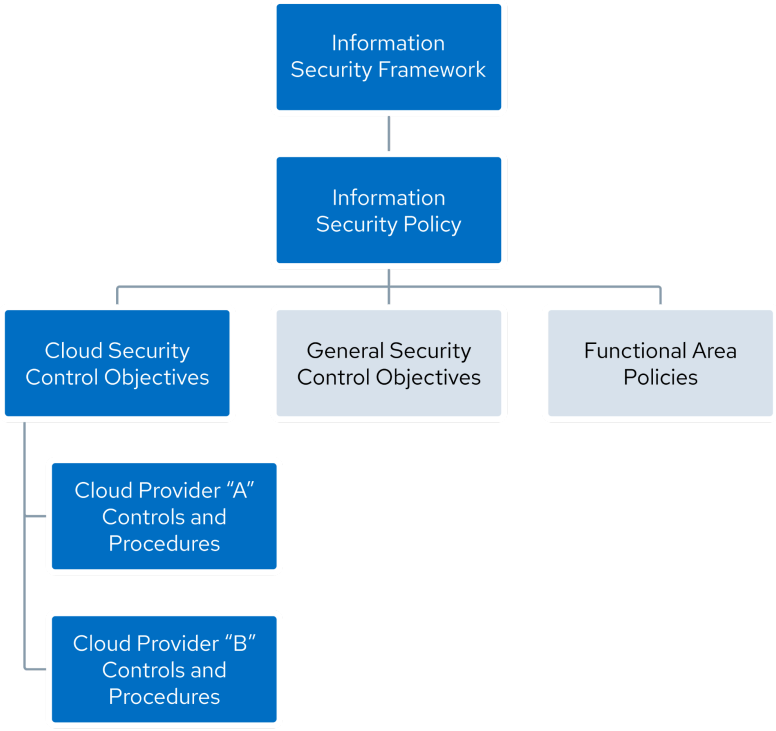

Figure 7: Structured Security Governance Hierarchy

2.2.1 Aligning with Requirements, Standards, Best Practices, & Contractual Obligations

To establish a robust governance framework, it is important to align with established standards, best practices, and contractual obligations.

Understanding the contractual obligations of your CSP is crucial to knowing the shared security responsibilities between your organization and the CSP, as well as any specific security requirements outlined in the contract. Additionally, consider contractual obligations with customers and partners, as they may impact your cloud plans.

Stay informed about current best practices. CSPs often provide recommended practices through their well-architected frameworks. While deviations may be necessary, these frameworks are valuable references for establishing a secure cloud environment.

2.2.2 Consulting with Key Stakeholders for Cloud Security Strategy Alignment

A non-exhaustive list of stakeholders to align with for cloud includes the IT department, security team, compliance and legal team, finance department, business unit leaders, development team, operations team, project management office, vendors and service providers, and end users.

2.3 Cloud Security Frameworks

A cloud security framework organizes and prioritizes security control objectives to achieve desired security outcomes. Frameworks categorize these objectives, enabling a systematic approach to cloud security.

Cloud-specific frameworks consider the unique characteristics of cloud computing, addressing aspects like on-demand resource allocation, shared responsibility models, and rapid elasticity. Using these frameworks ensures security programs align with cloud requirements and challenges.

There are many frameworks relevant to cloud security. The major examples are the CSA Cloud Controls Matrix (CCM)[9], ISO/IEC 27017:2015[10], BSI C5[11], NIST 800-53[12], Payment Card Industry Security Standards Council (PCI SSC) Cloud Computing Guidelines[13], NIST CSF V2[14], and the CSA Cloud Security Maturity Model (CSMM)[15].

For additional details about cloud frameworks, we recommend the Certificate of Cloud Auditing Knowledge (CCAK) course available through ISACA.

2.3.1 Cloud Controls Matrix

An example of a cloud-specific framework is the CSA Cloud Controls Matrix v4 (CCM v4), which is a library of control objectives that structures 17 control domains. It offers comprehensive coverage of a wide array of security topics, ranging from governance and risk management to operational security and data privacy. This makes it a valuable resource for organizations looking to enhance their cloud security.

One of the key strengths of the CCM is its alignment with leading standards, such as ISO/IEC 27001/27002, PCI Data Security Standard (DSS) (v3.2.1/v4.0), NIST, and so on. By harmonizing with

[9] CSA. (2024) Cloud Controls Matrix (CCM)
[10] ISO/IEC (2015) 27017:2015 - Information technology - Security techniques - *Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*
[11] BIS (2020) Federal Office for Information Security - *Cloud computing C5 criteria catalogue*.
[12] NIST (2020) SP 800-53 Rev 5 - *Security and Privacy Controls for Information Systems and Organizations.*
[13] PCI (2013) PCI Data Security Standard (PCI DSS) - *Information Supplement: PCI DSS Cloud Computing Guidelines.*
[14] NIST. (2024) The NIST Cybersecurity Framework (CSF) 2.0
[15] CSA (2023) Publication Peer Review - *Cloud Security Maturity Model 2023*.

these established frameworks, the CCM ensures that organizations can achieve compliance across multiple standards and regulations.

The CCM is tailored to cloud environments, making it well-suited for securing multi-tenant, distributed, and dynamic cloud systems. The focus on the unique challenges of cloud computing sets it apart from more generic security frameworks like NIST CSF. Additionally, the CCM allows for control customization, enabling organizations to adapt the security controls to their specific cloud architectures, delivery models (IaaS, PaaS, SaaS), and compliance needs.

Another key benefit of the CCM is its support for cloud governance. It assists organizations in establishing and maintaining a solid cloud governance program that effectively manages and oversees cloud risks. This is valuable in ensuring that cloud deployments are aligned with organizational objectives and comply with relevant regulations.

The CCM is continuously updated to reflect the latest cloud security best practices. Organizations can rely on the CCM as a reliable and relevant resource for their cloud security needs by staying up to date.

Based on the CCM, the Consensus Assessment Initiative Questionnaire (CAIQ) provides a checklist to evaluate controls.

2.3.2 CSA Security, Trust, Assurance, and Risk (STAR) Registry

The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. Cloud providers can submit completed CAIQ documents to the CSA STAR Registry. The CSA initiated this program to advance transparency and confidence in cloud services. The program offers a framework for CSPs to document their security practices and for CSCs to evaluate the security posture of cloud services.

The CSA STAR program[16] comprises two primary components:

1. **CSA STAR Certification:** This entails an independent third-party evaluation of a cloud service provider's security controls against the CSA Cloud Controls Matrix (CCM) and other recognized industry standards like ISO/IEC 27001. Achieving CSA STAR Certification indicates that a cloud service provider has implemented robust security measures and practices.

2. **CSA STAR Attestation:**[17] The CSA STAR Attestation is a collaboration between CSA and the AICPA[18] to provide guidelines for Certified Public Accounts (CPAs) to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. The STAR Attestation provides rigorous third party independent assessments of cloud. providers.

[16] Learn more about the STAR program at: https://cloudsecurityalliance.org/star
[17] Learn more about STAR Attestation requirements using CSA's *Guidelines for CPAs Providing CSA STAR Attestation*
[18] American Institute of Certified Public Accountants

By facilitating standardized security assessments and promoting transparency, the CSA STAR program empowers organizations to assess the security, privacy, and compliance practices of cloud service providers. This, in turn, helps them make risk-aware decisions when selecting and utilizing cloud services, fostering trust and reliability in the cloud industry.

2.4 Policies

Information security policies are crucial for establishing a strong security framework. They govern the protection of an organization's information assets, outline necessary control objectives, and should require business leadership sign-off to ensure alignment with strategic goals.

There are several key examples of information security policies organizations commonly implement:

- The Information Security policy is a top-level policy defining how the information security program will be run. It ideally refers to other policies and documents, such as control objectives, rather than trying to include all the specific technical requirements.
- Additional policies underneath the core policy that define specific areas, such as Acceptable use, data protection, identity management, endpoint and mobile device protections, use of cloud services, third-party risk management, and so on. There are many online sources of security policy libraries and templates from sites such as SANS Institute, and CIS.