Domain2 Cloud Governance and Strategies

ISACA defines **governance** as: ensures the evaluation of needs, conditions and options **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.

- Cost efficiency and speed to market are key drivers for cloud adoption.
- Accelerated deployment cycles introduce governance risks, such as misconfigurations ...
- Governance => **balance** between the **requirement for speed** and the need to **control risks**.

Two primary ways cloud affects security governance:

- The introduction of the **Shared Responsibilities Model**. The accountability of the control remains with the (CSP) or (CSC). **==Compliance risk** is always with the CSC.==
- The **technical** and **operational differences** (*created by the inherent nature of cloud computing.*)
- Most providers have a standard offering that cannot be customized according to all customer's specific requirements.
- 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 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
- (DevSecOps) drive **the automation of security controls,** which changes organizational structures. + Artificial Intelligence (AI) and Machine Learning (ML) + Zero Trust (ZT)

Governance Hierarchy:

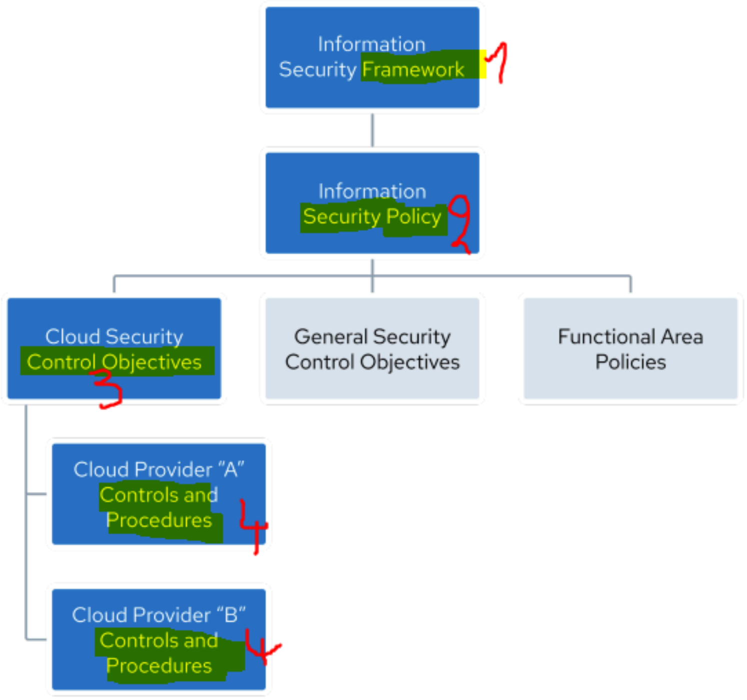
Information Security Framework
1
Information Security Policy
2
Cloud Security Control Objectives
3
General Security Control Objectives
Functional Area Policies
Cloud Provider "A" Controls and Procedures
4
Cloud Provider "B" Controls and Procedures
4

Figure 7: Structured Security Governance Hierarchy

1. **Sec Framework:**
    1. **Risk framework:** guidelines for evaluating cybersecurity risks (*NIST 800-30, ISO 27005, CIS RAM, and FAIR.*)
    2. **Program framework**: components of your security program (*NIST Cybersecurity Framework (CSF), ISO 27001, or Control Objectives for Information and Related Technology (COBIT*))
    3. **Control Frameworks**: technical and procedural controls (*NIST 800-53, Center for Internet Security Critical Security Controls (CIS CSC), and Cloud Security Alliance Cloud Controls Matrix (CSA CCM)*)
2. **Policies**: outline an organization's security requirements and should require business leadership sign-off to ensure alignment with strategic goals
3. **Control Objectives**: desired security control outcomes to minimize risk.
4. **Control Specifications**: Technical implementations **to meet control objectives.** (*enabling MFA for user access and applying a technical policy to enforce it.*)

- Understanding the contractual obligations of your CSP is crucial to knowing the shared security responsibilities between your organization and the CSP
- Stay informed about current best practices.

CSA Cloud Controls Matrix (CCM): v4 (CCMv4)

- Library of control objectives.
- Structures 17 control domains.
- **Key strengths**: alignment with leading standards, tailored to cloud environments, focus on the unique challenges of cloud computing, its support for cloud governance.
- the Consensus Assessment Initiative **Questionnaire** (CAIQ) provides a checklist to evaluate controls.

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

- a publicly accessible registry
- documents the security and privacy controls provided by popular cloud computing offerings.
- offers a framework **for CSPs to document their security practices**.
    - **CSA STAR Certification:** an independent **third-party evaluation** of a cloud service provider's security controls against the CCM
    - **CSA STAR Attestation:** a collaboration between CSA and the AICPA to provide guidelines for Certified Public Accounts (CPAs)+ third party independent assessments of cloud providers.