Domain 3: Risk, Audit and Compliance

This domain focuses on cloud security, risk, audit, and compliance. It covers evaluating cloud service providers and establishing cloud risk registries. It also discusses different types of compliance requirements and introduces tools and technologies to support cloud governance and risk management. Overall, it provides insights into managing the complex landscape of cloud computing risks and compliance.

Learning Objectives

In this domain, you will learn to:

- Define, categorize, and use tools to manage risk.
- Identify the regulatory and compliance constraints for which your cloud-based environment must undergo audits.
- Identify a set of technical and non-technical tools used when managing governance, risk, and compliance.

3.1. Cloud Risk Management

Effective cloud risk management is mandatory in today's digital landscape, where organizations increasingly rely on cloud services. This section delves into the importance of understanding cloud risks and provides insights on establishing a cloud risk profile, assessing cloud service providers, maintaining a cloud risk register, and conducting risk assessments, threat intelligence, and threat modeling.

3.1.1 Cloud Risks

Let’s start with an example. A company has a cloud storage bucket filled with personal information on customers. We call this an **asset**, which to an attacker (also known as a **threat actor**) is a **target**. One of the weaknesses of a cloud storage bucket is that it may be misconfigured. We call that a **vulnerability**, and to an attacker, this represents an **attack vector**.

A **risk** is that the personal data in the bucket leaks out, and the company gets fined by a regulator. Another risk could be that, through some action, the data becomes unavailable or corrupted.

A **control** or **countermeasure** is a way to reduce the risk. Typical controls here would be any policy that prevents these storage buckets from being accessible to the whole internet, or more specifically: the threat actor.

Ideally, we'll have enough controls to reduce the risk down to an acceptable level. This involves understanding what the important assets and threat actors are. This process is called **threat modeling** and is discussed in other places in this guidance, such as application security. Threat modeling, in a cloud world, starts with identifying the various places and cloud services where data is stored, and how data flows between them. See also CSA research[19].

The following examples show some of the most common risk factors and categories, both general and security risks. We also recommend reviewing the Cloud Security Alliance's *Top Threats*[20] research report. In the 2022 edition, the 'Pandemic Eleven', these were the top categories:

- Insufficient Identity, Credentials, Access, and Key Management
- Insecure Interfaces and APIs
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture and Strategy
- Insecure Software Development
- Unsecured Third-Party Resources
- System Vulnerabilities
- Accidental Cloud Data Disclosure
- Misconfiguration and Exploitation of Serverless and Container Workloads
- Organized Crime/Hackers/Advanced Persistent Threat (APT)
- Cloud Storage Data Exfiltration

There are many other sources of cloud threat intelligence. Consult the CSA website for up-to-date information. Additionally, the **MITRE ATT&CK®**[21] framework provides a comprehensive matrix of threat actor tactics.

3.1.2 Understanding Cloud Risk Management

Risk management involves a structured approach to identifying, assessing, and addressing risks associated with cloud computing. The risk management and methodologies used in cloud computing are not different from the ones adopted in the on-premises world and in other technologies, what does change are some of the specific actions taken during the definition of the scope and environment and the risk evaluation and treatment process.

The European Network and Information Security Agency (ENISA) *Risk Management Process*[22] provides a framework that organizations can adapt to manage these risks effectively within their cloud environments. This process is designed to be integrated into an organization's broader operational processes, ensuring a broad approach to risk management. Here's an expansion on the key components of this process.

[19] CSA. (2021) Publications: Cloud Threat Modeling
[20] CSA. (2021) Research Topic: Top Threats
[21] MITRE. (2024) Cloud Matrix
[22] ENISA. (2022) The Risk Management Process

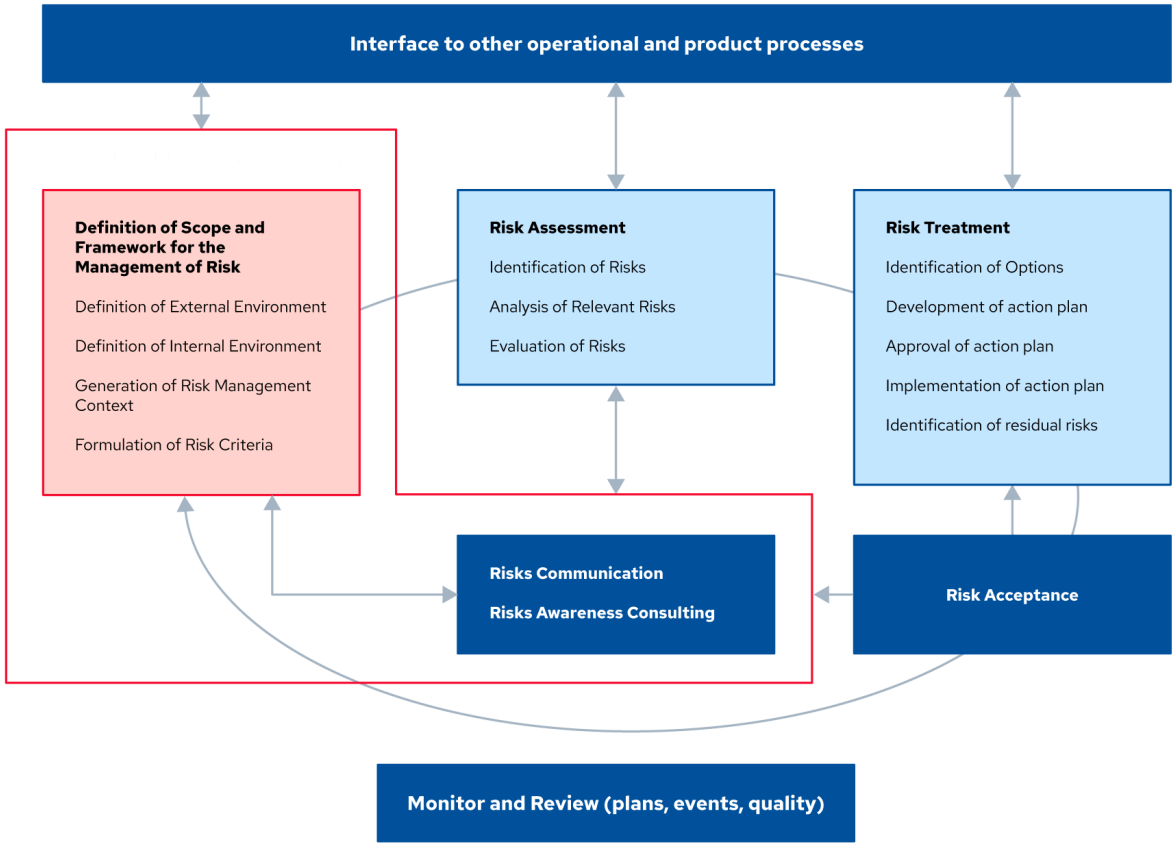

Figure 8: Comprehensive Cloud Risk Management Framework

3.1.2.1 Corporate Risk Management Strategy

These days, cloud usage serves a variety of corporate objectives with wildly varying risk appetites. The corporate risk management strategy sets the stage for risk management, in general, which helps translate business risk management to cloud risk management.

3.1.2.2 Risk Assessment

Identify and analyze relevant risks to understand their potential impact on the organization. This involves evaluating each risk to determine the likelihood of occurrence and the severity of its consequences.

3.1.2.3 Risk Treatment

After assessing risks, develop and approve an action plan to mitigate, transfer, avoid, or accept each risk. Implement these action plans and identify any residual risks that remain.

3.1.2.4 Interface to Other Operational & Product Processes

Risk management should not be siloed; it must interface with other business processes to ensure that risk considerations are embedded throughout the organization's operations and product lifecycle.

3.1.2.5 Monitoring & Review (Plans, Events, Quality)

Continuously monitor risk management plans, events, and the quality of risk management activities. Regular reviews ensure that risk management processes remain effective and adapt to any changes in the business environment.

3.1.3 Assessing Cloud Services

One of the first steps in managing cloud risks is having a systematic process to assess cloud providers and services. This assessment should align with your business needs and risk tolerance.
The following process is designed to account for these differences:

- Business requests
- Review CSP documentation
- Review external sources
- Map to compliance requirements
- Map to data classification
- Define required and compensating controls
- Approval process

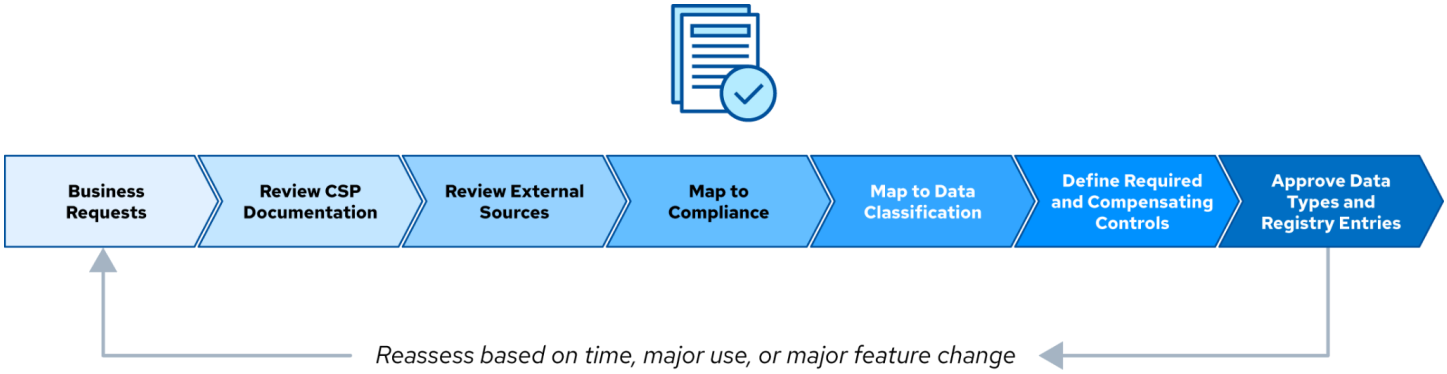

Figure 9: Systematic Process for Evaluating and Approving Cloud Services

3.1.3.1 Business Requests

Whether or not the business unit has a specific cloud service in mind, it is important to understand the business need and the data involved. This helps to understand risk appetite and any relevant policies and regulations.

3.1.3.2 Review CSP Documentation

Most CSPs have the following categories of documentation:

- **Security and privacy documentation:** Review the CSP's published security policies, privacy policies, and data handling practices to ensure they align with your organization's standards.
- **Service level agreements (SLA) and contracts**: SLAs outline the performance and uptime commitments of the CSP, while contracts detail the terms of service, including responsibilities and liabilities.
- **Terms of service (ToS):** Understanding the ToS is important to avoid legal or operational surprises post-adoption. These may be the only legal contracts between you and the provider.
- **CAIQ and certifications:** The CSA Consensus Assessments Initiative Questionnaire (CAIQ), based on the Cloud Controls Matrix (CCM) provides a comprehensive set of questions that CSPs answer to disclose their security controls. CSP certifications (e.g., ISO/IEC 27001, SOC 2) offer third-party validation of their security practices.

3.1.3.3 Review External Sources

Research: Investigate external reviews, reported vulnerabilities, and any past security and operational incidents involving the CSP to gauge their security posture and response capabilities.

3.1.3.4 Map to Compliance Requirements

When selecting a CSP, it is essential to align their features and policies with the organization's compliance needs, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or Payment Card Industry Data Security Standard (PCI DSS). This ensures that regulatory requirements are met and that the organization's data remains secure.

3.1.3.5 Map to Data Classification

Not all data needs the same risk management. Providers and services should be approved based on data types, which allows flexibility, so not all providers and services need to meet the same standards for the most sensitive data. It's acceptable to use a riskier service with less valuable or public data.

- **Data sensitivity assessment**: Assess the sensitivity of data in transit and at rest. Not all data carries the same risk; thus, not all cloud services are required to meet the highest security standards.
- **Service approval based on data type:** Approve CSPs and their services based on the classification of data they will handle. This approach allows for flexibility and efficient use of resources.

3.1.3.6 Define Required & Compensating Controls

Before final approval, security defines any required controls (e.g., configuration settings within the CSP) and any compensating controls (e.g., third-party tools) needed to use the service with the designated data types.

3.1.3.7 Approval Process

Based on the gathered information and mapping, decide whether the CSP's services are appropriate for the intended data types. If they meet all criteria, approve their use and incorporate them into the organization's cloud register, ensuring visibility and control over cloud adoption.

3.1.4 The Cloud Register

A cloud register is a central repository of approved cloud services, and what kind of data they are approved to handle at a given level of risk. This guides internal decisions on which providers and services to use for which projects. It also helps ensure that data is only used with compliant services, and thus plays a role in compliance as well.

Provider	Service	Data Types	Risk	Expiration
ABC	Object storage	Public, sensitive	Low	Annual
ABC	Virtual networks	All	Low	Annual
GHI	CRM SaaS	PII	Moderate	Quarterly

Table 1: Cloud Registry Example

This fictitious example shows three specific services from two providers and lists the data types that are allowed to be processed. Based on that, risk is assigned, and the required review frequency. This allows teams to accelerate risk assessment.

3.2 Compliance & Audit

Compliance is the adherence to a set of requirements stemming from internal policies, applicable laws and regulations, sector-specific codes of conduct and codes of practices, standards, and best practices. Complying with applicable requirements allows organizations to satisfy internal policies and code of ethics, safely operate in the market, and in some cases (e.g., adhere to international standards), gain a competitive advantage.

Compliance requirements can stem from:

- National and international standards and regulations can regulate the processing, storing, and transfer of certain types of data.
- Industry standards, such as PCI, for credit card handling. Many standards have cloud-specific guidance.
- Contracts.
- Internal policies and standards. These may need updating if they are too specific for on-premises environments.

Compliance is demonstrated through audits and conformity assessments that evaluate the suitability of the system of controls to satisfy the applicable requirements.

3.2.1 Jurisdictions

Many cloud deployments may span different legal and regulatory jurisdictions. The complexity of compliance becomes magnified when operations extend across multiple regions, each with its own legal and regulatory frameworks governing data privacy, security, and other critical factors. Let's delve deeper into the factors influencing jurisdictional considerations in the cloud environment.

Cloud providers and cloud consumers operating in multiple regions will face a matrix of jurisdictions where various laws and regulations apply. This is affected by:

- The location of the cloud provider.
- The location of the cloud consumer.
- The location of the data subject.
- The location where the data is stored.
- The legal jurisdiction of the contract, which may be different than the locations of any stakeholders.
- Any treaties or other legal frameworks between those various locations.

An example could be the requirement to issue a breach notification in the country you are operating in, even if the data was hosted in a different region.

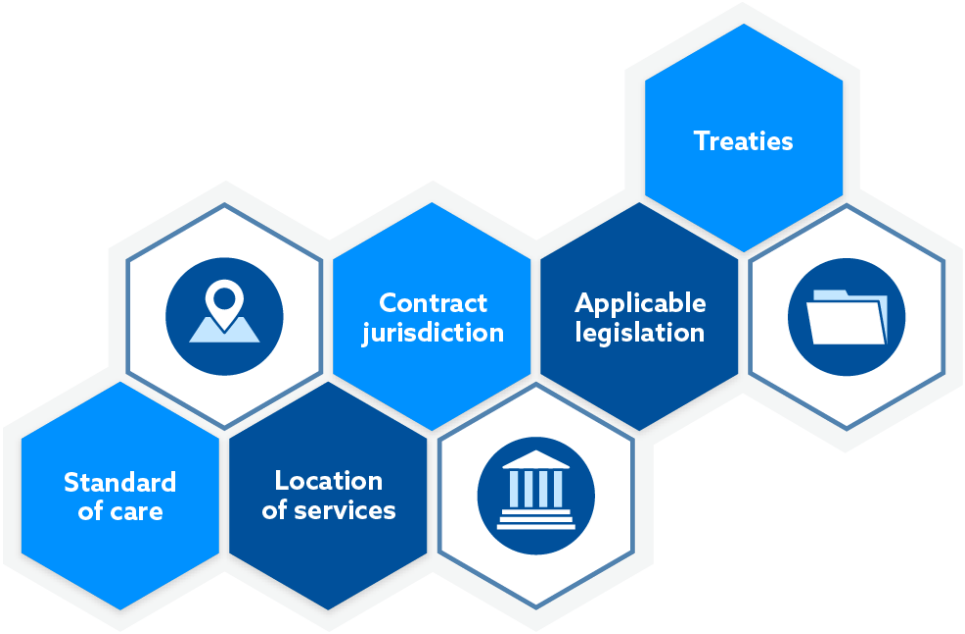

Figure 10: Factors Influencing Cloud Jurisdiction Compliance

3.2.2 Cloud-Relevant Laws & Regulations Examples

There are a myriad of laws and regulations to navigate, and each organization has the obligation to understand its own specific set of legal and regulatory requirements. The following are some representative examples of regulations and industry standards that commonly affect cloud security and compliance.

3.2.2.1 Privacy Laws & Regulation

- **EU GDPR:** Sets a high standard for data protection, emphasizing individuals' rights over their personal data, requiring consent for data processing, and imposing strict penalties for non-compliance.
- **US Regulations (CCPA/COPPA):** Focus on specific sectors, protecting
    - Children's Online Privacy (COPPA)
    - California Consumer Privacy Act (CCPA), and other State-level acts with detailed requirements for handling and safeguarding data
- **Brazil LGPD:** Stands for General Personal Data Protection Law in English, strongly based on the EU GDPR. Like European law, it also sets a high standard for data protection, emphasizing individuals' rights over their data, requiring consent for data collecting and processing, and imposing strict penalties for violations.

- **Japan Act on the Protection of Personal Information, Australian Privacy ACT:** National laws that regulate the collection, use, and disclosure of personal information, focusing on user consent, data accuracy, and cross-border data flow restrictions.

3.2.2.2 Other Relevant Laws & Regulations

- **US Regulations:**
    - Gramm-Leach-Bliley Act (GLBA), imposes requirements on financial institutions in the United States to protect consumer information.
    - Health information (HIPAA), safeguards medical privacy by establishing regulations on how healthcare providers, insurers, and others who handle data can use and disclose personal health information.
- **EU Laws and Regulations:**
    - EU Digital Operational Resilience Act (DORA), which ensures operational resilience for critical financial market infrastructures operating in public cloud platforms.
    - EU AI Act establishes essential regulations to ensure the trustworthiness of Artificial Intelligence (AI) systems.
    - NIS 2, the recently enforced update to the Network and Information Systems (NIS) Directive, strengthens cybersecurity measures for critical services across the EU
    - EU Cybersecurity Act aims to fortify the digital defenses of European Union institutions themselves.
    - EBA Guidelines on outsourcing arrangements by the European Banking Authority
- **Cybersecurity Law of the People's Republic of China:** Focuses on protecting the country's online infrastructure and data by outlining security obligations for companies, promoting public awareness of cyber threats, and granting authorities broad powers to monitor and regulate cyberspace.
- **Payment Card Industry Data Security Standard (PCI DSS):** A cross-jurisdictional standard for organizations that handle and process cardholder information, emphasizing financial data protection through comprehensive security measures.

3.2.2.3 Compliance in the Cloud

In general, some of the factors that are common across several laws and regulations are:

- **Secure handling:** Ensuring that access to sensitive data is tightly controlled and that data is processed to maintain its confidentiality and integrity.
- **Secure storage:** Implementing encryption and other protective measures to safeguard data at

rest and in transit, ensuring proper data retention and deletion practices.

- **Due care:** Adhering to industry best practices and security standards to protect data from threats and vulnerabilities.
- **Audit trails:** Maintaining comprehensive records of data processing activities to demonstrate compliance with regulatory requirements and facilitate audits.

3.2.2.4 Adherence to Standards

Cloud providers often achieve conformity against a variety of regulations, industry, and national standards through certifications, attestation, and other forms of authorization. The most important ones are as follows.

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process. ISO/IEC 27001 is designed to help organizations of any size or industry to protect their information systematically and cost-effectively by adopting a comprehensive set of information security controls and management practices.

System and Organization Controls (SOC) is a compliance standard for service organizations developed by the American Institute of CPAs (AICPA). It focuses on five Trust Service Criteria: security, availability, processing integrity, confidentiality, and privacy. SOC reports are designed to provide detailed information and assurance about a service organization's controls relevant to these criteria. It is particularly important for SaaS and technology companies that handle customer data to ensure they have the necessary controls in place to protect that data.

The Security Trust Assurance and Risk (STAR)[23] Registry was developed by the CSA. Through the STAR program, cloud providers can publish their adherence to these standards enhanced with cloud-specific controls from the CCM.

3.2.3 Compliance Inheritance

Cloud compliance typically follows a shared responsibility model, where the CSP and the CSC are each responsible for certain aspects of compliance. Compliance inheritance aims to relieve some of the burden on the customer by allowing the customer to acquire a control set from a compliant provider. Consider a cloud infrastructure provider who is PCI DSS-compliant. A customer using their infrastructure services will inherit this set of controls and will be PCI DSS-compliant at the infrastructure level. The customer, however, will be additionally responsible for ensuring that the software built on this infrastructure is also PCI DSS compliant. Both the CSP and CSC are audited independently, and each must ensure that all their respective controls are compliant.

[23] STAR is covered in greater detail in Domain 2: *Cloud Governance & Strategies*.

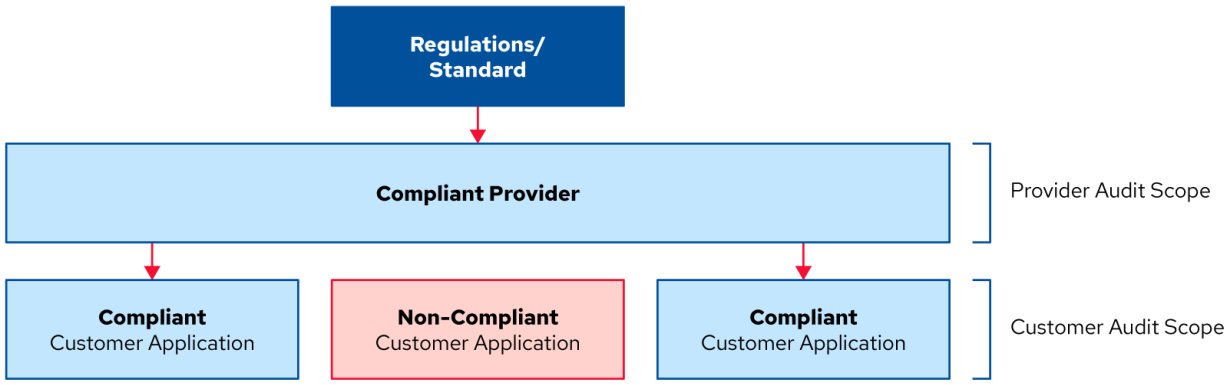

Figure 11: Audit Scope: Provider vs. Customer Responsibilities

3.2.4 Artifacts of Compliance

Compliance artifacts include the logs, documentation, and other materials needed for audits and compliance; they serve as evidence to support compliance activities. Customers are ultimately responsible for providing the necessary artifacts for their audits. Therefore, they need to understand what the provider offers and create their own artifacts to cover any gaps. For example, they might need to enhance the logging within an application if server logs on a PaaS platform are not accessible.

The following are examples of compliance artifacts:

- **Audit Logs:** These logs are detailed records of events, actions, and changes within the cloud environment.
- **Activity Reporting:** Reports summarizing user activities, access patterns, and system interactions. Activity reports can help identify unauthorized access, track user actions, and ensure that operational practices align with compliance requirements.
- **System Configuration Details:** Documentation of system configurations, including network settings, access controls, and security measures.
- **Change Management Details:** Records of changes made to the system, including updates, modifications, and patches. These details are critical for ensuring that changes are authorized, tested, and implemented in a manner that maintains the integrity and security of the environment.

3.3 Governance, Risk, Compliance Tools & Technologies

In the governance, risk, and compliance (GRC) tool kit, are technical and non-technical tools. This includes clear documentation of responsibilities, contracts, and repositories that store maintained risk

registers and service registries. The content can also be documentation describing frameworks and processes that have been adapted for their business context and adoption process for the teams across the organization. There is also a wide variety of technical tools that are used to automate tasks that would be too labor-intensive for humans to do using manual processes.

Many tools for implementing Governance, Risk, and Compliance are described throughout this Study Guide. Examples include the Shared Security Responsibility Model (Domain 1), contracts (Domain 3), risk register (Domain 3), cloud provider policies (Domain 4), and automation (Domains 5 and 10).