Domain 3 Risk, Audit and Compliance

Cloud Risks:

- A **control** or **countermeasure** is a way to reduce the risk.

Threat modeling:

- Understanding what the important assets and threat actors are.
- Places and cloud services where data is stored, and how data flows between them.
- The MITRE ATT&CK® framework provides a comprehensive matrix of threat actor tactics.
- 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 **provides a framework** .
- Risk management should not be soiled, it must interface with other business processes to ensure that risk considerations are embedded throughout the organization's operations and product life cycle.

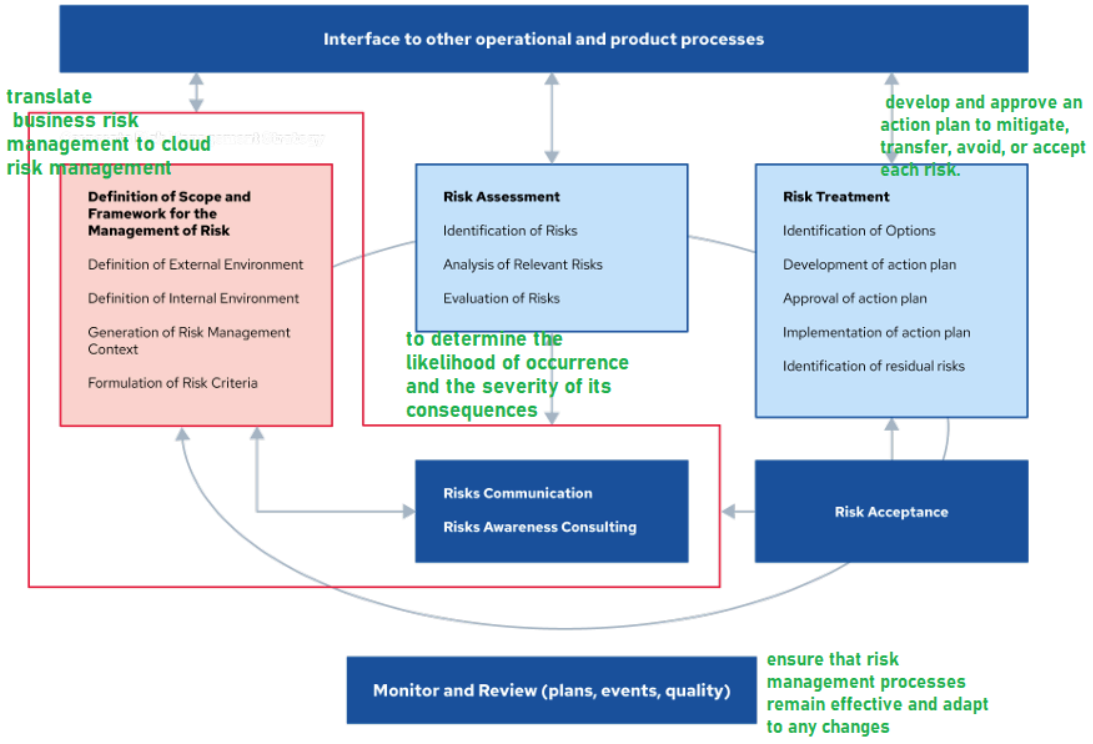

Figure 8: Comprehensive Cloud Risk Management Framework

- 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**.

Assessing Cloud Services:

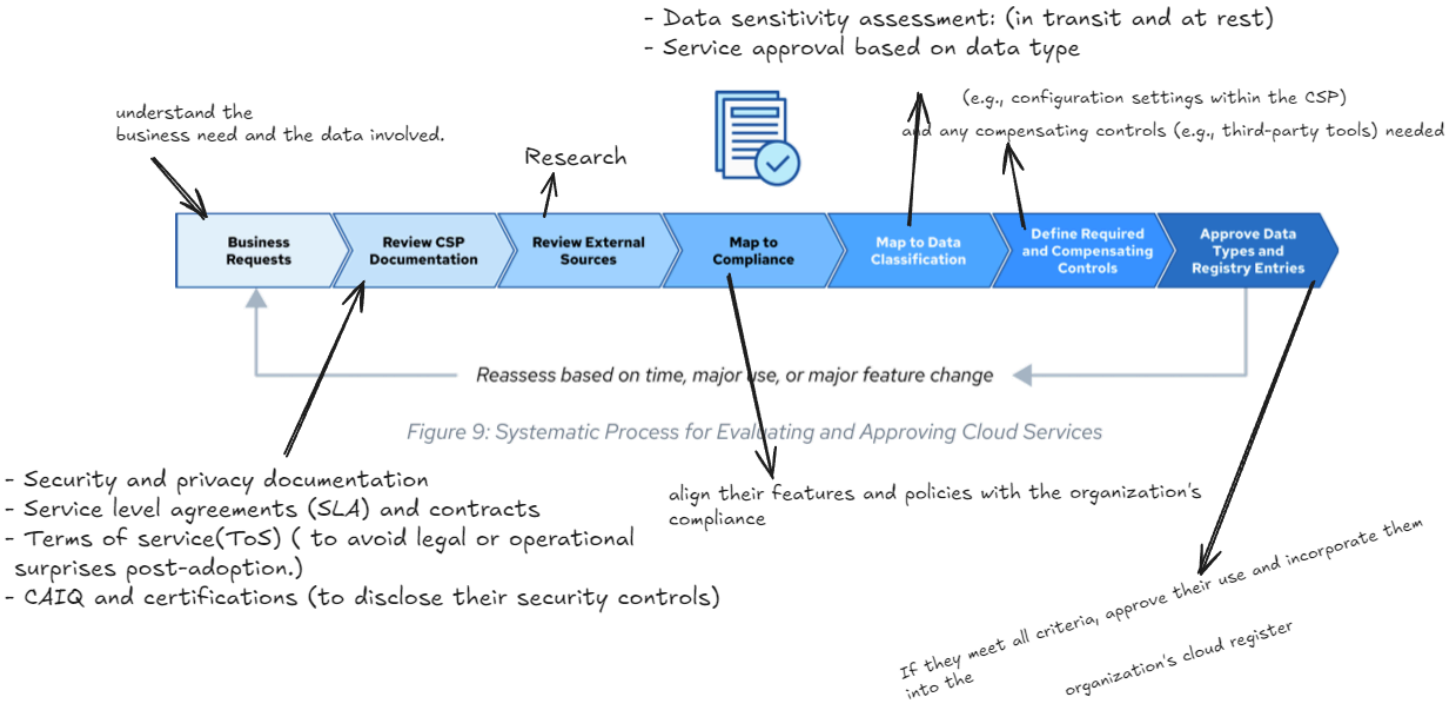

Figure 9: Systematic Process for Evaluating and Approving Cloud Services

The Cloud Register:

- is a central **repository of approved cloud services** + **data they are approved to handle** **at a given level of risk**

Provider	Service	Data Types	Risk	Expiration
ABC	Object storage	Public, sensitive	Low	Annual

- Risk is **assigned**.

Compliance & Audit

- Is the adherence to a set of **requirements**.
  - National and international standards and regulations
  - Industry standards.
  - Contracts.
  - Internal policies and standards.
- Compliance **standards factors**:
  - **Secure handling**: access to sensitive data is tightly controlled
  - **Secure storage**: encryption and other protective measures
  - **Due care**: Adhering to industry best practices
  - **Audit trails**: demonstrate compliance with regulatory requirements and facilitate audits.
- Compliance **artifacts**:
  - Audit Logs
  - Activity Reporting
  - System Configuration Details

    - Change Management Details

Jurisdictions are 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.

Privacy Laws & Regulation:

- EU **GDPR**: high standard for data protection.
    - EU Digital Operational Resilience Act (**DORA**): operational resilience for critical financial market infrastructures
    - **EU AI Act** : regulations to ensure the trustworthiness of Artificial Intelligence (AI)
    - **NIS 2**.
    - **EU Cybersecurity Act**.
    - **EBA** Guidelines: European Banking Authority outsourcing arrangements.
- **US Regulations (CCPA/COPPA)**: Children's Online Privacy (COPPA) + California Consumer Privacy Act (CCPA).
    - Gramm-Leach-Bliley Act (**GLBA**): requirements on financial institutions.
    - Health information (**HIPAA**): safeguards medical privacy.
- **Brazil LGPD**: Stands for General Personal Data Protection Law in English.
- **Japan Act on the Protection of Personal Information, Australian Privacy ACT.**
- **Cybersecurity Law of the People's Republic of China** .
- **PCI DSS**

Adherence to Standards

- **ISO/IEC 27001** is an **international standard** for information security management systems (ISMS).
- provides a systematic approach to managing sensitive company information so that it remains secure.
- **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**.
- The Security Trust Assurance and Risk (**STAR**).

Compliance inheritance:

- 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**.
- The CSP and CSC are **audited independently**.

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).