Governance & Regulation
Day 19/365

- **Governance**: Managing and directing an organisation or system to achieve its objectives and ensure compliance with laws, regulations, and standards.
- **Regulation**: A rule or law enforced by a governing body to ensure compliance and protect against harm.
- **Compliance**: The state of adhering to laws, regulations, and standards that apply to an organisation or system.

Information security governance falls under the purview of top-tier management and includes the following processes:

- **Strategy**: Developing and implementing a comprehensive information security strategy that aligns with the organisation's overall business objectives.
- **Policies and procedures**: Preparing policies and procedures that govern the use and protection of information assets.
- **Risk management**: Conduct risk assessments to identify potential threats to the organisation's information assets and implement risk mitigation measures.
- **Performance measurement**: Establishing metrics and key performance indicators (KPIs) to measure the effectiveness of the information security governance program.
- **Compliance**: Ensuring compliance with relevant regulations and industry best practices.

Governance and Regulation are linked but have different meanings, security regulations refer to legal and regulatory frameworks that govern the use and protection of information assets, they are designed to protect sensitive data form unauthorized access, theft and misuse. Compliance with regulations is mandatory and enforced by gov. agencies or regulatory bodies

Relevant Laws and Regulations
a common language for organisations to measure their security posture and ensure regulatory compliance. Following is an overview of some relevant laws and regulations:

Law/Regulation	Domain	Description
General Data Protection Regulation (GDPR)	Data Privacy & Protection	GDPR is a regulation propagated by the European Union that sets strict requirements for how organisations handle and protect and secure the personal data of EU citizens and residents.
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare	A US-based official law to maintain the sensitivity of health-related information of citizens.
Payment Card Industry Data Security Standard	Financial	Set technical and operational requirements to ensure the secure handling, storage, processing, and

(PCI-DSS)		transmission of cardholder data by merchants, service providers, and other entities that handle payment cards.
Gramm-Leach-Bliley Act (GLBA)	Financial	Financial companies must be sensitive to their customers' nonpublic personal information (NPI), including implementing information security programs, providing privacy notices, and disclosing information-sharing practices.

Frameworks

The information security framework provides a comprehensive set of documents that outline the organisation's approach to information security and governs how security is implemented, managed, and enforces within the organization. This includes

- Policies: A formal statement that outlines an organisation's goals, principles, and guidelines for achieving specific objectives.
- Standards: A document establishing specific requirements or specifications for a particular process, product, or service.
- Guidelines: A document that provides recommendations and best practices (non-mandatory) for achieving specific goals or objectives.
- Procedures: Set of specific steps for undertaking a particular task or process.
- Baselines: A set of minimum security standards or requirements that an organisation or system must meet.

Developing Governance Documents

Governance Risk and Compliance (GRC)

It is a holistic approach to information security that aligns with the organisation's goals and objectives and helps to ensure that the organisation operates within the boundaries of relevant regulations and industry standards. GRC framework has the following three components:

Privacy and Data Protection

Citizen's Personally identifiable information (PII)

General Data Protection Regulation (GDPR)

The GDPR is a data protection law implemented by the EU in May 2018 to protect personal data. Personal data is "Any data associated with an individual that can be utilised to identify them either directly or indirectly".

- **Prior approval** must be obtained before collecting any personal data.
- Personal data should be kept to a **minimum** and only collected when necessary.

- **Adequate measures** are to be adopted to protect stored personal data.

Key points

Companies can only collect personal data for a legitimate reason and must inform the owner about its processing, penalties and fines include:

- Tier 1: More severe violations, including unintended data collection, sharing data with third parties without consent, etc. Maximum penalty amounting to 4% of the organisation's revenue or 20 million euros (whichever is higher).
- **Tier 2**: Less severe violations, including data breach notifications, cyber policies, etc. The maximum fine for Tier 2 is 2% of the organisation's revenue or 10 million euros (whichever is higher).

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is focused on maintaining secure card transactions and protecting against data theft and fraud. It is widely used by businesses, primarily online, for card-based transactions. It was established by major credit card brands (Visa, MasterCard & American Express). It requires strict control access to cardholder information and monitoring unauthorised access, using recommended measures such as web application firewalls and encryption

---

NIST 800-53

NIST 800-53 is a publication titled "Security and Privacy Controls for Information Systems and Organisations" provides a catalogue of security controls to protect the CIA triad of information systems

ISO/IEC 27001

ISO 27001 is an internationally recognised standard for requirements to **plan, develop, run, and update** an organisation's Information Security Management System (ISMS).. It was developed by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has the following core components:

- **Scope**: This specifies the ISMS's boundaries, including the covered assets and processes.
- **Information security policy**: A high-level document defining an organisation's information security approach.
- **Risk assessment**: Involves identifying and evaluating the risks to the confidentiality, integrity, and availability of the organisation's information.
- **Risk treatment**: Involves selecting and implementing controls to reduce the identified risks to an acceptable level.
- **Statement of Applicability (SoA)**: This document specifies which controls from the standard are applicable and which are not.
- **Internal audit**: This involves conducting periodic audits of the ISMS to ensure that it is operating effectively.
- **Management review**: Review the performance of ISMS at regular intervals.


Benefits of ISO 27001
Reduce the chances of security breaches within your IT environment
Confidentiality of the information
Minimisation of IT risks, possible damage and consequential costs
Competitive edge due to recognised standard
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements
Fulfilment of internationally recognised requirements
Systematic detection of vulnerabilities
Lower costs
Control of IT risk