CYBERSECURITY COMPLIANCE

JAWAD ALI

Cybersecurity Compliance

Difference Between:

1. **Standard**
2. **Policy**
3. **Law**
4. **Regulation**
5. **Compliance**

Standard	Policy	Law	Regulation	Compliance
Standards provide guide on how to implement certain controls.	Policy is the rule created by the organization management for smoothing their operations.	It is a rule that is created by the government body and is legally enforced within that country.	A regulation is a detailed requirement that tells us how to comply with the law.	Compliance is the act of following laws, regulations, standards, and policies that apply to an organization.
It is created by the industry bodies or the organization.	It is created by the organization.	It is created by the government bodies.	It is created by the government agencies.	Compliances are usually created by a state.
For example, ISO 27001 is a standard.	For example, an organization may have a password policy in place.	For example, GDPR is a law.	For example, EPA created regulations to enforce environmental laws.	For example, if an organization follows GDPR, then it is GDPR compliant.

Compliance:

Definition:

In simple words, compliance is adhering to every law, regulation, and ethical guideline that applies to a certain organization.

Working:

First, standards are set for an organization at the top level, and the organization tries to meet those standards. If an organization fails to meet those standards, it is called failure or lack of compliance which leads to penalties and other consequences depending on the severity and the

scale of the problem. Mostly failure of compliance leads to financial penalties, sometimes it also leads to reputational damage. Good compliance provides a vast amount of fundamental support for an organisation, ensuring it retains integrity and effective strategic planning. Without these things, a company runs the risk of severe damage.

ISO 27001:

ISO 27001 is an international standard for establishing, implementing, and maintaining an Information Security Management System (ISMS) to protect an organization's data.

Use:

ISO 27001 helps organizations to systematically protect their information assets. This is achieved by risk assessment and risk treatment.

Region:

It is an international standard that is used on a global level.

Organization Responsible for Creation:

ISO 27001 was created jointly by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission).

Industries on which it is Applicable:

There is not specific industry that needs to follow ISO 27001. Every industry that wants to manage information security risks can adopt ISO 27001.

Core Requirements:

- Organization needs to understand its context and scope and determine the scope of ISMS.
- Top management needs to make a security policy and be responsible for ISMS.
- Identify and evaluate risks and make risk treatment plan.
- Allocate resources, train employees, and maintain documented information.

Real World Importance:

- ISO 27001 makes an organization credible.
- It ensures effective resource allocation.
- It gives a structure framework for compliance and audit.
- It reduces the possibility and damage of a breach, which is essential for business continuity.

Reference Link:

https://en.wikipedia.org/wiki/ISO/IEC_27001

NIST Cybersecurity Framework:

NIST Cybersecurity framework is a set of guidelines that helps organizations manage and reduce risk.

Use:

NIST framework is used by the organizations that want to assess, manage, and improve cybersecurity risks.

Region:

It is a US guideline, but it is adopted worldwide.

Organization Responsible for Creation:

It was created by NIST (National Institute of Standards and Technology) which is a US institute.

Industries on which it is Applicable:

Originally it was designed for critical infrastructure such as telecom, water electricity, and transportation but now every type of industry can use NIST framework.

Core Requirements:

- There are six core functions of NIST framework Govern, Identify, Protect, Detect, Respond, and Recover that are divided into categories and subcategories.
- Current and target profiles are made so that it can determined that where the organization stands currently and where it wants to be.

Real World Importance:

- It tells the organizations what their risk management maturity level is.
- It promotes continuous improvement.
- Every organization can customize it according to their size, resource and threat environment.

Reference Link:

https://www.nist.gov/

PCI-DSS:

PCI DSS is the Payment Card Industry Data Security Standard, a set of security standards that any organization must follow to securely process, store, or transmit credit and debit card information.

Use:

PCI-DSS (Payment Card Industry Data Security Standard) was made to protect payment card data. It defines technical and operational security controls so that data of the cardholder stays safe.

Region:

It is a global standard because card payment industry operates globally.

Organization Responsible for Creation:

It was created by PCI Security Standards Council (PCI SSC) which includes major card brands (Visa, Mastercard, American Express, Discover, JCB).

Industries on which it is Applicable:

The companies that store, process or transmit cardholder data need to follow this standard.

Core Requirements:

- Install and maintain Firewall and Network Security.
- Do not use vendor supplied default passwords.
- Protect the stored cardholder's data.
- Encrypt the data transmission.
- Unique Ids for users.
- Malware protection and regular updates.
- Need to know the access control.

Real World Importance:

- If an organization is not PCI-DSS compliant, the payment processors or acquiring banks can impose penalties or stop the card payments from that organization.
- In case of breach of the cardholder data, the losses would be massive.
- It increases the transparency and trust.

Reference Link:

https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/pci-dss-requirements/

GDPR:

GDPR, or the General Data Protection Regulation, is a European Union regulation that harmonizes data privacy and protection laws across Europe.

Use:

GDPR is a data protection and privacy law that wants to protect the personal data of individuals and guides the organization on how to collect, store, process and share data.

Region:

It is a regulation of European Union (EU) and European Economic Area (EEA).

Organization Responsible for Creation:

European Parliament and Council of the European Union were responsible for passing this regulation.

Industries on which it is Applicable:

Every organization that processes the data of the data subjects in EU or EEA whether that organization is in technology, healthcare, e-commerce, finance, education or any other sector must follow GDPR. If a non-European Union company is serving EU citizens, it must follow GDPR.

Core Requirements:

- Embed data protection principles while designing products and processes.
- Take explicit consent from data subjects and provide clear information to them regarding the use of their data.
- People have the right to access data, rectification, erasure, data portability, and objection.
- Data only the data that is necessary.
- Implement technical and organizational measures.
- In case of a breach, it is necessary to inform the supervisory authority within 72 hours.

Real World Importance:

- GDPR has set a new standard regarding data in the world. Many companies all around the world follow GDPR in their operations.
- It makes the organization think seriously about the cyber risk and data handling because of the high fines.
- It increases customer trust because they know their will not be misused.

Reference Link:

https://gdpr.eu/what-is-gdpr/

HIPAA:

HIPAA, or the Health Insurance Portability and Accountability Act of 1996, is a US law that sets national standards to protect sensitive patient health information from being disclosed without the patient's consent.

Use:

HIPAA is a US federal law that regulates Protected Health Information **PHI** with privacy and security rules and standardizes electronic health transactions.

Region:

It is a US law. HIPAA is for US citizens and non-US citizens alike, as long as they are receiving care or their protected health information is handled by a covered entity in the United States.

Organization Responsible for Creation:

US Congress passed this act in 1996, and later US Department of Health and Human Services (HHS) defined Privacy Rule, Security Rule, and Enforcement Provisions.

Industries on which it is Applicable:

Healthcare providers (hospitals, clinics), health planners (insurance companies), and associates that handle PHI must follow HIPAA if they are US based.

Core Requirements:

- It requires administrative, technical, and physical controls to protect ePHI (electronic Protected Health Information).
- In case of a breach, the organization must inform the affected individuals and HHS.
- Healthcare providers must be allotted NPI (National Provider Identifier).

Real World Importance:

- HIPAA ensures that data of the patient is secured which develops trust between patients and healthcare organizations.
- The violations have very costly consequences (investigations, lawsuits, civil money penalties).
- Its compliance can save organizations from lawsuits, data breaches, and reputational damage.

Reference Link:

https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html