

Q.1

Ans:- As the Chief Information Security Officer (CISO) of a mid-sized financial services company expanding into the European Union (EU), ensuring strong data security governance and compliance with the General Data Protection Regulation (GDPR) became a critical responsibility.

① Key principle of Data Security Governance and their Application:-

⇒ Data Security governance provides the framework through which an organization ensure effective oversight of the data protection responsibilities. The key principles includes accountability, Transparency, risk-based control, Compliance and Continual improvement.

② Steps to ensure GDPR and Regulatory Compliance:-

⇒ To meet GDPR and similar regulations, a phased strategy should be adopted:

- i) Conduct a data protection Impact Assessment (DPIA).

- ii) Appoint a Data protection Officer (DPO):

- iii) Update data processing Agreements (DPAs):

- iv) Implement the rights of the data subjects.

- v) Establish a lawful basis for processing.

- vi) Ensure Breach notification procedures.

3) The role of risk assessment and data classification:

a) Risk assessment:-

⇒ Conducting a comprehensive risk assessment helps identify vulnerabilities across system, application, and processes.

Using framework like NIST SP 800-30, Categorize risk based

on likelihood and impact, and apply appropriate controls

Example:- If employees are accessing PII via unsecured third-party tools, this would be a high-risk area requiring immediate mitigation.

B). Data Classification:- Introduce a data classification policy to categorize information (e.g.: Public, Internal, Confidential, Restricted).

This ensures:-

- Proper handling of personally identifiable information (PII)
- Enforced encryption standards (e.g., AES-256 for restricted data).
- Tiered access control based on sensitivity.

4). Managing Shadow IT and third-party Vendor Controls.

⇒ Shadow IT, unapproved use of cloud services poses compliance, security, and financial risk. A multifaceted strategy is essential.

a). Visibility and Discovery:-

⇒ Use tools like CASBs. CASBs (Cloud Access Security Brokers) (e.g. Microsoft Defender for cloud Apps, Netskope) to detect and monitor unauthorized SaaS usage.

B). Centralized Procurement and approval process:

⇒ Enforce a strict policy where all technology acquisitions are routed through IT and information security teams for vetting and security check.

C). Third-party risk management framework:

⇒ Leverage ISO 27036 for Vendor Security assurance. Implement regular vendor audits, security questionnaires and require SOC 2 type 1 or ISO 27001 certificates.

D) Zero trust approach:-

⇒ Adopt the zero trust security never trust, always verify for all users and devices. This reduces risks from unmanaged endpoints accessing company data.

E) Building a Culture of Security Awareness and Accountability.

⇒ A security framework cannot succeed without an engaged and aware workforce. Cultivating this culture requires the following:-

- a). Regular security training and Phishing Simulation.
- b). Clear policies and enforcement.
- c). Executive Support and modelling.
- d). Security Champions program.

• Conclusion:-

⇒ Establishing effective data security governance in a financial institution entering the EU market involves more than compliance. It requires strategic alignment with global best practices, robust risk management, and a security first mindset.