

Compliance Checklist

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation:

- Evaluate if ABC International Bank processes personal data of European Union (EU) citizens.
- Assess compliance with GDPR requirements, including data protection, privacy rights, and breach notification obligations.
- Verify if the bank has processes in place to inform affected individuals within 72 hours in case of a data breach.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation:

- Determine if ABC International Bank stores, accepts, processes, or transmits credit card information.

- Verify compliance with PCI DSS requirements to ensure a secure environment for handling credit card data.

ISO 27001

ISO 27001 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization. It sets out the criteria for assessing the security risks and implementing controls to protect the confidentiality, integrity, and availability of information assets.

Explanation:

- Consider implementing ISO 27001 as a framework for information security management.
- Evaluate if ABC International Bank has established and maintains a comprehensive set of security controls based on ISO 27001 standards.

NIST Cybersecurity Framework (CSF):

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a widely recognized and widely adopted framework that provides organizations with a flexible and comprehensive approach to managing and improving their cybersecurity posture.

Explanation:

- Assess if ABC International Bank has adopted the NIST CSF as a guideline for managing and mitigating cybersecurity risks.
- Evaluate if the bank has implemented the core functions (Identify, Protect, Detect, Respond, Recover) and associated controls outlined in the framework.

By conducting this compliance checklist, ABC International Bank can ensure it meets the relevant regulatory requirements, protects customer data, and establishes a robust security posture in line with GDPR, PCI DSS, ISO 27001, and NIST CSF.