Read the security management frameworks and then answer the relevant questions.

ISO/IEC 27001

ISO/IEC 27001 is a globally recognized standard that provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO 27001 enables organizations of all sizes and sectors to systematically manage sensitive information, ensuring its confidentiality, integrity, and availability. At its core, ISO 27001 adopts a risk-based approach to information security, requiring organizations to identify information security risks and select appropriate controls to mitigate them. The standard does not mandate specific technical measures but provides a management structure that integrates information security into the organization's overall processes and management structure. A key component of ISO 27001 is the establishment of a security policy, clear assignment of responsibilities, ongoing staff training, asset management, access control, cryptography use, physical and environmental security, operations security, communications security, system acquisition and development, supplier relationships, incident management, business continuity management, and compliance with legal requirements.

Organizations pursuing ISO 27001 certification must undergo rigorous internal and external audits. Certification provides independent verification that an organization's ISMS meets the international standard, which can strengthen trust with customers, partners, and regulators. Beyond compliance, ISO 27001 fosters a culture of continuous improvement through the "Plan-Do-Check-Act" (PDCA) cycle, ensuring that security measures are regularly evaluated and improved in response to evolving threats. In a world increasingly dependent on information technology and digital data, ISO 27001 is crucial. It provides assurance that an organization is effectively managing the risks associated with information assets, not only protecting business interests but also safeguarding customer and stakeholder trust.

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was developed in response to a U.S. presidential executive order that called for a standardized approach to managing cybersecurity risks. Initially designed for critical infrastructure sectors, the NIST CSF has since been widely adopted across industries worldwide due to its practical, flexible, and scalable structure. The NIST CSF organizes cybersecurity activities into five core functions: Identify, Protect, Detect, Respond, and Recover. The "Identify" function focuses on gaining a comprehensive understanding of the organizational context, resources, and cybersecurity risks to manage systems, assets, and data effectively. "Protect" involves developing and implementing safeguards to limit or contain the impact of a potential cybersecurity event. "Detect" requires the development and implementation of activities to identify the occurrence of a cybersecurity event. "Respond" involves taking appropriate action regarding a detected event, and "Recover" is about maintaining plans for resilience and restoring any impaired capabilities or services.

Unlike regulatory standards, the NIST CSF is voluntary, allowing organizations to tailor its recommendations based on size, risk appetite, and sector. It emphasizes a risk-based approach and promotes continuous improvement by encouraging organizations to move from a reactive to a proactive cybersecurity posture. It bridges communication between technical experts and executive leadership, aligning cybersecurity activities with business requirements and risk tolerance. The NIST CSF serves as a roadmap to building a cybersecurity program from scratch or improving an existing one, making it a vital tool in today's digital economy, where cyber threats are rapidly evolving and increasingly sophisticated.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized standard that governs the security of cardholder data. Established by the Payment Card Industry Security Standards Council (PCI SSC)—a collaboration between major credit card brands such as Visa, MasterCard, American Express, Discover, and JCB—PCI DSS aims to protect cardholder data from breaches and fraud. PCI DSS applies to all organizations that store, process, or transmit cardholder data. The standard outlines 12 major requirements categorized into six control objectives: building and maintaining a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy. Specific measures include installing firewalls, encrypting data transmissions, restricting access to cardholder data, and conducting vulnerability assessments. Compliance with PCI DSS is validated either through Self-Assessment Questionnaires (SAQs) or by a formal audit conducted by a Qualified Security Assessor (QSA), depending on the organization’s transaction volume. Non-compliance can result in significant fines, higher transaction fees, and reputational damage.

Beyond compliance, PCI DSS is essential for maintaining customer trust in e-commerce and retail transactions. As cyber threats evolve, so does PCI DSS, with periodic updates reflecting new risks and technologies. Organizations that prioritize PCI DSS compliance not only secure their payment environments but also demonstrate a broader commitment to data security best practices.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a landmark U.S. federal legislation that protects sensitive patient health information from being disclosed without the patient's knowledge or consent. Administered by the Department of Health and Human Services (HHS), HIPAA establishes national standards for the protection of individually identifiable health information, known as protected health information (PHI).

HIPAA is composed of several rules. The Privacy Rule sets standards for the use and disclosure of PHI and gives individuals rights over their health information, including rights to examine and obtain a copy of their health records and request corrections. The Security Rule outlines technical and non-technical safeguards that organizations must implement to secure electronic PHI (ePHI). The Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases, the media, when a breach of unsecured PHI occurs. HIPAA applies to covered entities, which include healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates who handle PHI. Compliance with HIPAA requires administrative, physical, and technical safeguards, such as risk assessments, workforce training, access controls, encryption, and regular audits.

Violations of HIPAA can result in substantial civil and criminal penalties. However, compliance is not solely about avoiding penalties; it is about building a culture of patient trust, improving data handling practices, and ensuring that healthcare organizations are resilient against increasingly sophisticated cyber threats targeting sensitive health information.

Q1:

In a company certified with ISO 27001, an employee accidentally sends a sensitive file to an external party. How should ISO 27001 controls handle this incident?

Q2:

If a third-party vendor storing customer data is breached, what ISO 27001 controls apply?

Q3:

An audit finds unauthorized devices connected to the company's internal network. How should ISO 27001 compliance address this?

NIST CSF — 3 Scenario-Based Questions and Answers

Q1:

A company detects malware spreading within its network. Which NIST CSF functions should be activated?

Q2:

During a third-party risk audit, missing security patches are found on vendor software. How does NIST CSF recommend handling it?

Q3:

An employee bypasses the VPN to access internal systems remotely. How does NIST CSF address this?

PCI DSS — 3 Scenario-Based Questions and Answers

Q1:

A retail store discovers skimming devices attached to POS terminals. What should they do under PCI DSS?

Q2:

An e-commerce company is breached via a vulnerability in a payment page script. What PCI DSS requirement addresses this?

Q3:

How can PCI DSS help prevent stolen credentials from being used at payment portals?

HIPAA — 3 Scenario-Based Questions and Answers

Q1:

A nurse accesses a celebrity's medical record without authorization. What does HIPAA require the hospital to do?

Q2:

A ransomware attack locks a hospital's patient database. How should the hospital respond under HIPAA?

Q3:

Telehealth sessions are found transmitting patient data without encryption. What HIPAA requirements are violated?