ICSI MODULE 11:

ISO Standards

11.1 ISO Standards

The International Organisation for Standardization creates standards for a wide range of topics. There are hundreds of such standards, and it would be impossible to cover them in a single chapter. In fact, each standard could be the subject of a chapter, or at least a few chapters. Some of the more important standards for network security are listed here:

- **ISO/IEC 15408:** The Common Criteria for Information Technology Security Evaluation
- **ISO/IEC 25000:** Systems and Software Engineering
- **ISO/IEC 27000:** Information technology — Security Technology
- **ISO/IEC 27001:** Information Security Management
- **ISO/IEC 27005:** Risk Management
- **ISO/IEC 27006:** Accredited Certification Standard
- **ISO/IEC 28000:** Specification for security management systems for the supply chain
- **ISO 27002:** Information Security Controls
- **ISO 27003:** ISMS Implementation
- **ISO 27004:** IS Metrics
- **ISO 27005:** Risk management
- **ISO 27006:** ISMS certification
- **ISO 27007:** Management System Auditing
- **ISO 27008:** Technical Auditing
- **ISO 27010:** Inter-organisation communication
- **ISO 27011:** Telecommunications
- **ISO 27033:** Network security
- **ISO 27034:** Application security
- **ISO 27035:** Incident Management
- **ISO 27036:** Supply chain
- **ISO 27037:** Digital forensics
- **ISO 27038:** Document reduction
- **ISO 27039:** Intrusion prevention
- **ISO 27040:** Storage security
- **ISO 27041:** Investigation assurance
- **ISO 27042:** Analysing digital evidence
- **ISO 27043:** Incident Investigation

NIST Standards

11.2 NIST Standards

The U.S. National Institute of Standards and Technology establishes standards for a wide range of things. Some of the standards most important to network security are discussed in this section.

11.2.1 NIST SP 800-14

Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, describes common security principles that should be addressed within security policies. The purpose of this document is to describe 8 principles and 14 practices that can be used to develop security policies. This standard is based on 8 principles, which are:

1. Computer security supports the mission of the organisation.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. System owners have security responsibilities outside their own organisations.
5. Computer security responsibilities and accountability should be made explicit.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer is security is constrained by societal factors.

11.2.2 NIST SP 800-35

NIST SP 800-35, Guide to Information Technology Security Services, is an overview of information security. In this standard six phases of the IT security life cycle are defined:

- **Phase 1: Initiation.** At this point the organisation is looking into implementing some IT security service, device, or process.
- **Phase 2: Assessment.** This phase involves determining and describing the organisation's current security posture. It is recommended that this phase use quantifiable metrics.
- **Phase 3: Solution.** This is where various solutions are evaluated and one or more are selected.
- **Phase 4: Implementation.** In this phase the IT security service, device, or process is implemented.
- **Phase 5: Operations.** Phase 5 is the ongoing operation and maintenance of the security service, device, or process that was implemented in phase 4.
- **Phase 6: Closeout.** At some point, whatever was implemented in phase 4 will be concluded. Often this is when a system is replaced by a newer and better system.

11.2.3 NIST SP 800-30 Rev. 1

NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, is a standard for conducting risk assessments. Risk assessments were discussed in a previous chapter. This standard provides guidance to how to conduct such an assessment. There are nine steps in the process:

STEP 1. System Characterization
STEP 2. Threat Identification
STEP 3. Vulnerability Identification
STEP 4. Control Analysis
STEP 5. Likelihood Determination
STEP 6. Impact Analysis
STEP 7. Risk Determination
STEP 8. Control Recommendations
STEP 9. Results documentation

General Data Protection Regulation (GDPR)

11.3 General Data Protection Regulation (GDPR)

This is a European Union law first created in 2016. Its entire purpose is to deal with data privacy. It applies to any entity (business, government agency, etc.) that either collects data or processes that data. Even if an organisation is not within the EU, if it has EU data, then GDPR applies.

PCI DSS

11.4 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle cardholder information for the major credit and debit cards such as VISA and MasterCard. This industry regulation has several goals and the most important are listed below:

1.1 Requirement: All merchants must protect cardholder information by installing a firewall and router system. Installing a firewall system provides control over who can access an organisation's network and a router is a device that connects networks, and is therefore, PCI compliant.

Program the standards of firewall and router to:

1. Perform testing when configurations change
2. Identify all connections to cardholder information
3. Review configuration rules every six months

Configure firewall to prohibit unauthorised access from networks and hosts and deny direct public access to any information about the cardholder. Additionally, install firewall software on all computers that access the organisation's PCI compliance network.

1.2 Requirement: Change all default passwords. Default passwords provided when first setting up software are discernible and can be easily discovered by hackers to access sensitive information.

2.1 Requirement: Cardholder data is any personal information about the cardholder that is found on the payment card and can never be saved by a merchant—this includes preserving encrypted authentication data after authorization. Merchants can only display the maximum of the first six and last four digits of the primary account number (PAN). If a merchant stores PAN, ensure that the data is secure by saving it in a cryptographic form.

2.2 Requirement: It is required that all information is encrypted when transmitting the data across public networks, such as the Internet, to prevent criminals from stealing the personal information during the process.

3.1 Requirement: Computer viruses make their way onto computers in many ways, but mainly through e-mail and other online activities. The viruses compromise the security of personal cardholder information on a merchant's computer, and therefore antivirus software must be present on all computers associated on the network.

3.2 Requirement: In addition to antivirus software, computers are also susceptible to a breach in the applications and systems installed on the computer. Merchants must install vendor-provided security patches within a month of their release to avoid exposing cardholder data. Security alert programs, scanning services, or software may be used to signal the merchant of any vulnerable information.

4.1 Requirement: As a merchant, you must limit the accessibility of cardholder information. Install passwords and other security measurements to limit employees' access to cardholder data. Only employees who must access the information to complete their job are allowed to access the information.

4.2 Requirement: In order to trace employees' activities when accessing sensitive information, assign each user an unreadable password used to access the cardholder data.

4.3 Requirement: Monitor the physical access to cardholder data; do not allow unauthorised persons the opportunity to retrieve the information by securing printed information as well as digital. Destroy all outdated cardholder information. Maintain a visitor log and save the log for at least three months.

5.1 Requirement: Keep system activity logs that trace all activity and review daily. The information stored in the logs is useful in the event of a security breach to trace employee activities and locate the source of the violation. Record entries reflect at a minimum: the user, event, date and time, success or failure signal, source of the affected data, and the system component.

5.2 Requirement: Each quarter, use a wireless analyser to check for wireless access points to prevent unauthorised access. Also, scan internal and external networks to identify any possible vulnerable areas in the system. Install software to recognise any mod ification by unauthorised personnel. Additionally, ensure that all IDS/IPS engines are up to date.If you process credit cards, it is imper ative that you comply with this standard.

QUIZ:

- 1.Which U.S. standard covers risk assessment?
- 2.NIST SP 800-30 Rev.1 is a standard for conducting risk assessments.
- 3.What standard should you consult for managing incident response?
- 4.PCI DSS is a proprietary information security standard for organisations that handle cardholder data.
- 5.What does the Step 3 in NIST 800-30 Rev.1 clarifies?
- 6.Which of the following describes ISO 27003?
- 7.Which standard defines Management System Auditing?
- 8.Which U.S. standard should you consult to guide you in developing security policies?
- 9.What is the acronym of GDPR?
- 10.ISO 27035 describes incident management.