Unite V: Information Security Policy, Standards and Practices

Basic Concepts and Definitions

- **Information Security Policy:** A formal, high-level document that defines management's commitment to security, outlines objectives, and assigns responsibilities. It's the foundation of an organization's security program.
- **Standard:** Mandatory, specific rules or requirements that support a policy (e.g., "All passwords must be at least 12 characters").
- **Procedure:** Step-by-step instructions for implementing policies and standards (e.g., "Steps to reset a user password").
- **Guideline:** Recommended best practices that are not mandatory but offer guidance (e.g., "It is recommended to use a passphrase").
- **Baseline:** The minimum level of security required across all systems.
- **Framework:** A structured set of guidelines, like ISO 27001 or NIST, used to build and manage security policies.

Categories of Policies

A. Enterprise Information Security Policy (EISP)

- **Definition:** A high-level, strategic document that sets the overall direction, scope, and objectives for security across the entire organization.
- **Purpose:** To state management's commitment, define roles, and align security with business goals.
- **Example:** *"All employees must protect confidential data. Security is everyone's responsibility."*
- **Advantages:**
  - Provides top-level management endorsement.
  - Establishes a universal security culture.
  - Forms basis for detailed policies.
- **Disadvantages:**
  - Too broad for direct implementation.
  - Requires supporting documents to be effective.

B. Issue-Specific Information Security Policy (ISSP)

- **Definition:** Focuses on a specific topic or issue (e.g., email usage, remote access, social media).
- **Purpose:** To provide detailed rules for specific risks or technologies.
- **Structure:** Often includes scope, responsibilities, acceptable/unacceptable use, and compliance measures.
- **Example:** *"Remote Access Policy: All remote connections must use VPN and multi-factor authentication."*
- **Advantages:**
  - Clear, actionable rules for specific areas.
  - Easier to update and communicate.
- **Disadvantages:**
  - May become outdated quickly with technology changes.
  - Can lead to policy proliferation if not managed.

C. System-Specific Information Security Policy (SysSP)

- **Definition:** Technical policies for specific systems, devices, or platforms (e.g., firewall rules, server configurations).
- **Purpose:** To enforce security controls at the system level.
- **Forms:**
  - **Access Control Lists (ACLs):** Rule sets for network devices.
  - **Configuration Rules:** Settings for servers, databases, etc.
- **Example:** *"Firewall Policy: Block all inbound traffic on port 23 (Telnet)."*
- **Advantages:**
  - Provides precise technical enforcement.
  - Reduces human error in configuration.
- **Disadvantages:**
  - Highly technical; requires skilled staff.
  - May not align with business objectives if created in isolation.

The ISO 27000 series is a family of international standards from ISO/IEC providing a framework for Information Security Management Systems (ISMS) to help organizations protect data, manage risks, and build trust, with **ISO 27001** being the core standard for ISMS requirements and certification, alongside others like **ISO 27002** (guidelines) and specialized ones for cloud (27017) or risk (27005). It offers best practices for handling

sensitive information (financial, IP, customer data) for any organization size, focusing on people, processes, and technology to ensure security.

Key Standards in the Series

- **ISO 27000:** Provides an overview, terminology, and fundamental concepts for the entire family.
- **ISO 27001:** Specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS; it's the certifiable standard.
- **ISO 27002:** Offers detailed guidelines and best practices for implementing the controls mentioned in ISO 27001.
- **ISO 27005:** Focuses specifically on information security risk management.
- **ISO 27017:** Provides guidelines for information security controls in cloud computing services.
- **ISO 27018:** Addresses protection of Personally Identifiable Information (PII) in public clouds.

Purpose and Benefits

- **Systematic Approach:** Helps organizations manage security through a systematic risk management framework.
- **Data Protection:** Protects valuable assets like financial data, intellectual property, and customer information.
- **Risk Reduction:** Helps organizations stay ahead of cyber threats and data security risks.
- **Trust & Compliance:** Demonstrates commitment to security, building customer trust and aiding compliance with regulations like GDPR.
- **Universally Applicable:** Relevant to organizations of all sizes and industries.
    - **Advantages:**
        - Internationally recognized, boosts trust.
        - Comprehensive, covers people, process, technology.
        - Promotes continuous improvement (Plan-Do-Check-Act cycle).
    - **Disadvantages:**

    - Certification can be costly and time-consuming.
    - May be seen as bureaucratic for small organizations.
- **Example:** A bank uses ISO 27001 to build its ISMS, undergoes audit, and receives certification to assure customers of data safety.
- NIST Security Model
- NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.
- We can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

Identify

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:

Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.

Steps to take to protect against an attack and limit the damage if one occurs.

2. Protect

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.

- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

3. Detect

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

Investigate any unusual activities on your network or by your staff.

Check your network for unauthorized users or connections.

4. Respond

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly

5. Recover

After an attack:

Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

- **Key Publications:**
  - **NIST Cybersecurity Framework (CSF):** Core: Identify, Protect, Detect, Respond, Recover.
  - **NIST SP 800-53:** Security and privacy controls for federal systems.
  - **NIST SP 800-37:** Risk Management Framework (RMF).
- **Advantages:**
  - Flexible, scalable, and practical.
  - Publicly available (free).
  - Aligns well with regulatory requirements.
- **Disadvantages:**
  - Can be complex to implement fully.
  - Originally designed for US government; may need adaptation.
- **Example:** A healthcare provider uses NIST CSF to assess gaps in protecting patient data and plan improvements.

IETF Security Architecture

The **IETF Security Architecture** is not a single document or product, but a comprehensive framework of protocols, standards, and principles developed by the **Internet Engineering Task Force (IETF)** to secure communication across the Internet.

Rather than being a "top-down" rigid blueprint, it is a modular collection of standards (RFCs) that work together to provide five core security services: **Confidentiality, Integrity, Authentication, Access Control,** and **Non-repudiation.**

1. Core Framework Components

The architecture is generally divided into three functional layers that manage how security is applied to data:

Component	Description	Example Protocols

Component	Description	Example Protocols
Security Policy	Rules defining *what* needs protection and *how* (e.g., "all traffic to the HR server must be encrypted").	Security Policy Database
Security Protocols	The actual mechanisms that encapsulate and protect data at different layers of the OSI model.	IPsec, TLS, SSH
Key Management	Systems for safely exchanging cryptographic keys and establishing "trust" between parties.	IKEv2, PKI (X.509)

2. Key Architectural Pillars

The IETF approaches security by embedding it into different layers of the network stack, ensuring "Defense in Depth."

A. Network Layer Security (IPsec)

Defined primarily in **RFC 4301**, IPsec provides security at the IP level. It allows two nodes to communicate securely without the applications themselves needing to know anything about encryption.

- **AH (Authentication Header):** Ensures data integrity and origin authentication.
- **ESP (Encapsulating Security Payload):** Provides confidentiality (encryption) plus everything AH does.
- **Modes:** It operates in **Transport Mode** (host-to-host) or **Tunnel Mode** (gateway-to-gateway, used in VPNs).

B. Transport Layer Security (TLS)

TLS (the successor to SSL) is the most widely used part of the architecture. It secures communication between applications (like your browser and a web server).

- **Handshake Protocol:** Negotiates cipher suites and authenticates the server.
- **Record Protocol:** Handles the actual encryption and transmission of data.

C. Application Layer Security

Specific protocols designed for individual use cases:

- **S/MIME & PGP** (Secure/Multipurpose Internet Mail Extensions)**:** For securing email.
- **DNSSEC (Domain Name System Security Extensions):** To prevent DNS spoofing by digitally signing DNS records.
- **SNMPv3** (Simple Network Management Protocol version 3)**:** For secure network management.

3. The Concept of Security Associations (SA)

A fundamental concept in the IETF architecture is the **Security Association (SA)**.

An SA is a "contract" between two parties that defines which security services, keys, and algorithms will be used to protect their communication.

Before any data is sent, the parties use a key management protocol (like **IKEv2** (Internet Key Exchange version 2) to agree on the SA parameters. This ensures both sides are "speaking the same language" regarding encryption.

4. Fundamental Design Principles

The IETF follows specific philosophies when building these architectures:

- **Modular Design:** You can upgrade an encryption algorithm (e.g., moving from **AES-CBC** (Cipher Block Chaining) to **AES-GCM** (Galois/Counter Mode) without rewriting the entire protocol.
- **End-to-End Security:** Whenever possible, security should be handled by the endpoints (the sender and receiver) rather than middle-boxes in the network.
- **Open Standards:** All protocols are publicly reviewed (RFCs **(Request for Comments)**) to ensure no "backdoors" exist and to promote global interoperability.
- **Agility:** The architecture is designed to be "cryptographically agile," meaning it can quickly adapt as older algorithms (like MD5 (Message Digest 5)or SHA-1(Secure Hash Algorithm 1)) become insecure.

- **Advantages:**
  - Provides foundational standards for internet security.
  - Open, vendor-neutral, and widely implemented.
- **Disadvantages:**
  - Slow standardization process.
  - Optional adoption can lead to inconsistent security.
- **Example:** An e-commerce site implements TLS 1.3 to encrypt customer transactions, as per IETF standards.