Intro to Information Security

Unit – 1 Overview of Information Security

1. Information:

- Information is ***processed data*** that has meaning and context.
- It can be in the form of text, numbers, graphics, sound, video, or other formats that convey knowledge or facts.

2. Information Security

- Information Security is the ***practice of protecting information and the systems*** that store, process, and transmit it from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Objective to ensure the ***Confidentiality, Integrity, and Availability (CIA)*** of data.

3. CIA Triangle

The CIA Triad is the foundational model of Information Security that ensures protection of information assets through three key principles:

Confidentiality:

- Ensures that information is accessible only to authorized individuals.
- Prevents unauthorized disclosure of data.
- Achieved using:
  - Encryption (e.g., AES, TLS)
  - Access controls
  - Data classification
- Example: Encrypting user passwords in a database.

Integrity:

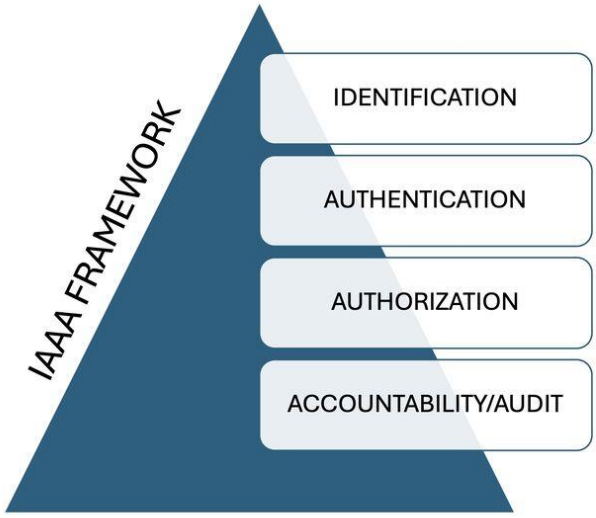
- Ensures that information remains accurate, consistent, and trustworthy.
- Protects against unauthorized modifications.
- Achieved using:
  - Hashing (e.g., SHA-256)
  - Digital signatures
  - Change control mechanisms
- Example: Verifying file integrity using hash values.

Availability:

- Ensures that information and systems are accessible to authorized users when needed.
- Prevents service disruptions.
- Achieved using:
  - Redundant systems (RAID, backups)
  - Load balancing
  - Failover systems
- Example: A backup server takes over during a hardware failure.

The CIA Triad forms the core of any security policy. All security measures should aim to balance and enforce these three principles.

4. IAAA:



5. Non-Repudiation:

- Non-repudiation is a security principle that ensures a sender cannot deny having sent a message, and a receiver cannot deny having received it.
- It provides proof of origin and delivery using digital signatures or logs, so that neither party can later claim, “I didn’t send/receive that.”
- Example: When you send an email with a digital signature, the recipient can prove it came from you, and you cannot deny sending it.

6. Security Concepts and their Relationships:

Vulnerability :

- A vulnerability is a ***weakness*** in a system that can be exploited by attackers.
- It can exist in software, hardware, people, or processes.
- Example: An outdated web server with unpatched software is vulnerable to known attacks.

Threat :

- A threat is ***any potential danger*** that can exploit a vulnerability.
- Threats can be intentional (hackers, malware) or accidental (human errors, natural disasters).
- Example: A hacker attempting to break into a network is a threat.

Risk:

- Risk is the possibility of loss or damage when a threat exploits a vulnerability
- It combines the likelihood of an attack and the impact it would cause.
- Example: If a weak password is a vulnerability and a brute-force attack is the threat, the risk is unauthorized access.

Exposure:

- Exposure refers to the state of being vulnerable to a threat due to lack of protection
- It shows how much of a system is open to attack.
- Example: If a database is connected to the internet without encryption, it is exposed.

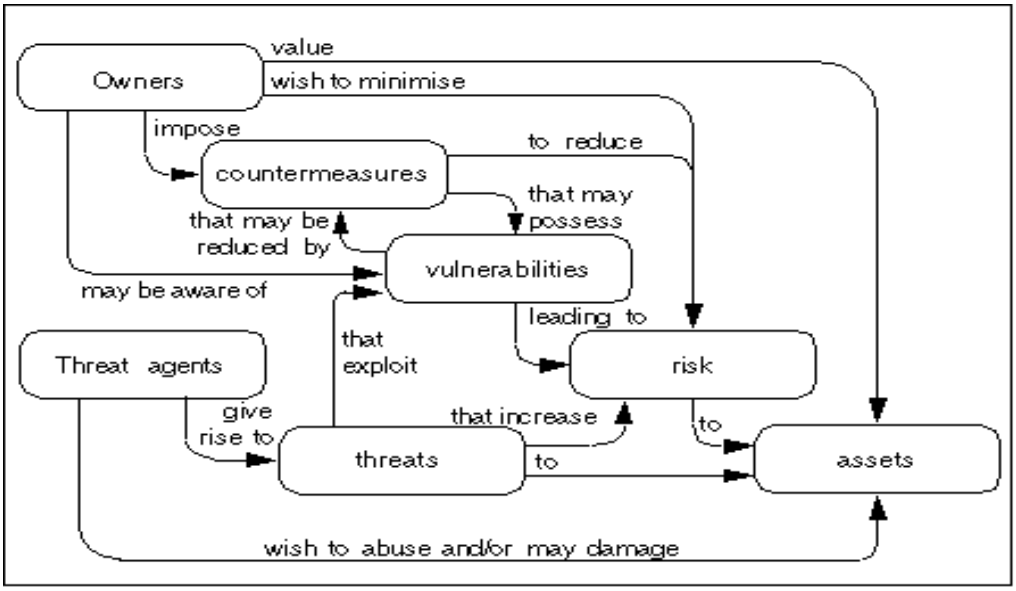
Control:

- A control is a safeguard or countermeasure that reduces risk.
- Controls can be technical (firewalls), physical (locks), or administrative (policies).
- Example: Using antivirus software is a control against malware threats.

Summary:

- Vulnerability: Weakness
- Threat: Potential attacker or danger
- Risk: Chance of damage from threat exploiting vulnerability
- Exposure: Level of openness to threats
- Control: Action or tool to reduce or prevent risk

Relationship:



1. Malicious Code:

1. Virus

- A **virus** is a type of malicious software that **attaches itself to a file or program** and spreads **when the file is executed**.
- It requires **human action** to spread (like opening an infected file).
- It can corrupt or delete data, slow down systems, or damage programs.
- **Real-world analogy:** Like a biological virus that needs a host to survive and spread.

---

2. Worm

- A **worm** is a self-replicating malware that **spreads automatically** across networks **without user interaction**.
- It consumes network bandwidth and can install other malware.
- Unlike viruses, worms do **not** need to attach to other files.
- **Example:** The "ILOVEYOU" worm spread rapidly via email.

---

3. Rootkit

- A **rootkit** is a type of malware designed to **hide its presence** and the presence of other malicious programs.
- It gives attackers **root or administrator-level access** to a system.
- Rootkits are hard to detect and often disable security tools.
- **Use case:** Attackers use rootkits to maintain long-term hidden access.

---

4. Trojan Horse

- A **Trojan Horse** looks like a **legitimate program** but contains hidden malicious code.
- It tricks users into installing it (like fake software or games).
- Once inside, it can steal data, give control to hackers, or install more malware.
- **Real-world analogy:** Like the mythological Trojan Horse used to sneak soldiers into Troy.

5. Backdoor

- A **backdoor** is a hidden entry point into a system that **bypasses normal authentication**.
- It may be intentionally created by developers or secretly installed by attackers.
- Used by hackers to access systems **remotely and repeatedly** without being noticed.
- **Danger:** Often used with Trojans or Rootkits to maintain access.

---

6. Polymorphic Threats

- **Polymorphic malware** can **change its code or appearance** every time it runs, making it hard to detect.
- Traditional antivirus tools struggle to recognize it because the malware keeps **"mutating."**
- It retains the same behavior (e.g., data theft) but disguises its signature.
- **Analogy:** Like a criminal who keeps changing their disguise to avoid capture.

---

2. Denial of Service:

A **Denial of Service (DoS)** attack is a cyberattack where the attacker attempts to make a system, network, or service unavailable to legitimate users by overwhelming it with excessive requests or malicious traffic.

Types of DoS Attacks:

1. **Simple DoS:**
    - Originates from a single machine.
    - Sends overwhelming traffic to exhaust server resources like CPU, RAM, or bandwidth.
2. **Distributed Denial of Service (DDoS):**
    - Attack is launched from multiple compromised systems (botnet).
    - Much harder to trace and more powerful.
    - Common attack vectors: SYN Flood, ICMP Flood, DNS Amplification.

How DoS Works:

- Sends continuous, fake, or malformed requests to a server.
- Exhausts system resources so it cannot respond to real users.
- Can crash websites, apps, or entire networks.

Example:

- A banking website is targeted by a DDoS attack that floods it with traffic, causing downtime and financial loss.

Consequences:

- Loss of service availability
- Financial damage
- Reputational loss
- Legal/regulatory consequences (especially for essential services)

Prevention & Mitigation:

- Use of firewalls and intrusion detection/prevention systems (IDS/IPS)
- Rate limiting and filtering
- Load balancing and redundant infrastructure
- DDoS protection services (e.g., Cloudflare, Akamai)

---

3. Social Engineering

Social engineering is a psychological manipulation technique used by attackers to trick people into giving away confidential information or performing actions that compromise security. It is a **non-technical attack** that targets **human behavior** rather than software or hardware.

How It Works:

- Attackers exploit trust, fear, curiosity, or urgency.
- The goal is to bypass technical security measures by deceiving humans.
- Can be carried out in person, via email, phone, or social media.

Common Social Engineering Techniques:

1. **Phishing:**
    - Fake emails or messages pretending to be from trusted sources.
    - Trick users into clicking malicious links or entering credentials.
2. **Spear Phishing:**
    - Targeted phishing aimed at a specific person or organization.
    - Often uses personalized details to increase trust.
3. **Whaling:**
    - Targets high-profile individuals like CEOs, CFOs (the "big fish").
    - Aim is to steal sensitive financial or strategic data.
4. **Pretexting:**
    - Attacker creates a fake identity and scenario to gain trust and extract information.
5. **Baiting:**
    - Leaves physical devices like infected USBs in public hoping someone plugs it in.
6. **Tailgating:**
    - Follows authorized personnel into restricted areas without permission.

Example:

An attacker phones an employee pretending to be an IT technician and asks for their login credentials to “fix a server issue.” The employee, trusting the caller, reveals the password.

Prevention Measures:

- User awareness training
- Multi-factor authentication (MFA)
- Verification of unexpected requests
- Strict access control policies
- Simulated phishing campaigns to educate employees

4. Security Policies:

Definition of Security Policy:

A **security policy** is a formal set of rules and guidelines that dictate how an organization protects its information assets. It defines expected behavior, responsibilities, and enforcement procedures to ensure the **Confidentiality, Integrity, and Availability (CIA)** of data.

Importance of Security Policies:

- Aligns security with business goals (mission, vision, strategy)
- Protects information from threats and misuse
- Establishes legal accountability and regulatory compliance
- Guides users, administrators, and systems in secure behavior
- Sets the foundation for standards, procedures, and guidelines

---

NIST Classification: The Three-Tier Policy Model

According to **NIST SP 800-14**, security policies are classified into three tiers:

Tier 1: Enterprise Information Security Policy (EISP) – Organization Level

- Also known as **General Security Policy**
- Sets the **strategic direction**, scope, and tone of the entire security program
- Typically written by senior management or the Chief Information Officer (CIO)
- Covers:
    - Organization's philosophy on information security
    - Responsibilities for employees, contractors, and third parties
    - Compliance requirements (legal, regulatory)
    - Risk tolerance and enforcement methods

Example: Defines how the company will protect its overall IT infrastructure, assign security roles, and maintain compliance with laws.

Tier 2: Issue-Specific Security Policies (ISSP) – Functional Level

- Focuses on **specific security issues** or technologies
- Provides rules for acceptable use and safeguards for each topic
- Updated frequently due to evolving threats
- Covers areas like:
    - Internet and email use
    - Use of personal devices
    - Antivirus and malware protection
    - Password policies

Example: A policy restricting USB device usage in office computers.

Tier 3: Systems-Specific Policies (SysSP) – Application/Device Level

- Technical policies and configuration rules for specific systems
- Includes access control lists, encryption settings, and audit procedures
- Directed at system administrators and engineers
- Can be in the form of scripts, templates, or procedural documents

Example: A SysSP for a database server detailing user access roles, backup procedures, and patch management.

Requirements for a Legally Enforceable Policy:

1. **Dissemination** – Must be accessible to all employees
2. **Review** – Must be understandable by all, including non-technical users
3. **Comprehension** – Users must prove understanding (e.g., quizzes)
4. **Compliance** – Users must agree (click-through, signed forms)
5. **Uniform Enforcement** – Policy must apply to all equally

5. Security Policy

- A high-level document that outlines the organization's **approach to protecting information assets**.
- Sets the foundation for the entire information security program.
- Defines acceptable behavior, responsibilities, and enforcement.
- Approved by top management.

Example: An enterprise-wide password policy that mandates password complexity.

---

6. Standards

- **Mandatory rules** derived from policies.
- Ensure consistency and uniformity across systems and departments.
- Define specific technologies, configurations, and operational requirements.

Example: All passwords must use at least 12 characters with uppercase, lowercase, numbers, and symbols.

---

7. Procedures

- **Step-by-step instructions** for implementing policies and standards.
- Targeted at operational staff (e.g., IT, system admins).
- Ensure that security actions are repeatable and consistent.

Example: The procedure to reset a user's password securely.

---

8. Guidelines

- **Recommended practices** (not mandatory).
- Offer flexibility and allow discretion depending on the situation.
- Help staff make informed decisions in non-standard situations.

Example: Recommended encryption practices for sending sensitive emails.

---

9. Baselines

- Define the **minimum acceptable level of security**.
- Used to compare and measure actual configurations.
- Helps in auditing and compliance checks.

Example: All workstations must have antivirus software, firewall enabled, and OS updated within 7 days.

Unit – 4 Information Asset Classification

---

1. Why should we classify information? Explain with its stake holders, how information is an asset (10 Marks)

Information is a valuable organizational asset that must be classified and protected based on its sensitivity, value, and impact. Classification helps determine appropriate security measures for confidentiality, integrity, and availability.

Why Classify Information?

1. To Protect Sensitive Data:
    - Ensures that confidential or critical data receives the right level of protection.
    - Prevents unauthorized access, misuse, or leakage.
2. Regulatory & Legal Compliance:
    - Certain data (like health or financial data) must meet compliance standards like GDPR, HIPAA, etc.
3. Efficient Resource Allocation:
    - Not all data needs the same level of protection.
    - Helps prioritize protection based on value and risk.
4. Supports Risk Management:
    - Helps identify where the highest information security risks lie.
    - Assists in applying correct controls.
5. Facilitates Access Control:
    - Only authorized stakeholders access certain categories of data.
    - Minimizes insider threats and accidental leaks.

Information as an Asset:

- Like money, infrastructure, and intellectual property, information has value.
- It supports:
    - Decision-making

    - Operational continuity
    - Competitive advantage
    - Brand reputation
- Loss or compromise of information can lead to:
    - Financial losses
    - Legal consequences
    - Reputational damage

Key Stakeholders in Information Classification:

Stakeholder	Role
Owner	Determines classification level, accountable for data integrity
Custodian	Implements protection measures, maintains backups, controls access
User	Accesses and uses data as per policy
Management	Defines classification policy and ensures enforcement
Security Team	Audits classification implementation, identifies risks

---

Common Information Classification Levels:

Level	Description	Example
Secret	Highest sensitivity, major damage if exposed	Military files, top-level strategy
Confidential	Harmful if disclosed	Financial records, client data
Private	Personal use, limited access	Employee files, internal emails
Public	Open to everyone	Website content, marketing brochures

Classifying information is essential to protect it based on value and sensitivity. It ensures that all stakeholders know their role in managing data securely and that security resources are applied efficiently. As a core component of governance, classification converts data into a protected, managed asset.

2. Three Key Stakeholders in Information Asset Management:

1. Asset Owners

- Senior individuals responsible for managing the security, lifecycle, and legal use of information assets.
- They decide:
  - What data is held and used
  - Who can access it and why
  - What protection levels are required
- They assess and report on security annually to support audits.

Example: A department head managing student records is the asset owner for that data.

---

2. Custodians

- Individuals responsible for the hands-on technical protection of the asset.
- They implement controls as directed by the owner.
- Duties include:
  - Data backups and restorations
  - Patch management
  - Antivirus configuration
  - Physical transport security (e.g., USB drives or CDs)

Example: An IT staff member deploying a secure backup system on the owner's instructions.

---

3. Users

- Authorized individuals who use information assets to perform organizational duties.
- Must follow all policies, procedures, and standards.
- Responsible for:
  - Preventing data misuse
  - Following password and access policies
  - Participating in awareness training

Example: A university employee accessing HR software must not share credentials or store sensitive data insecurely.

3. Information Classification

Information Classification is the process of categorizing information based on its sensitivity, value, and impact of disclosure. It helps determine the security controls needed to protect different types of data.

Classification Levels:

Level	Description	Example
🔐 Top Secret	Highest level; unauthorized access causes exceptionally grave damage to national security	Military operations, nuclear codes
🔐 Secret	Unauthorized disclosure could cause serious damage to national security	Defense strategies, diplomatic plans
🔒 Confidential	Highly sensitive data limited to users with a legitimate need-to-know; explicit authorization needed	PCI data, SOX compliance documents
🛡️ Private	Internal use only; exposure can have significant negative impact on the organization	Employee records, internal communications
📎 Official	Information used in routine government or business operations; requires moderate protection	Administrative documents, project plans
🗂️ Unclassified	Not a true classification level; data not needing protection or already declassified	Archived public records
🌐 Public	Intended for general public access; no legal restrictions	Press releases, marketing materials

---

Purpose of Classification:

- Helps apply appropriate controls based on sensitivity
- Reduces risk of data breaches
- Ensures regulatory compliance
- Enables access control (e.g., only authorized users access “Confidential” data)

Declassification & Reclassification:

- Declassification: Downgrading the classification when data no longer requires protection
- Reclassification: Upgrading or changing classification based on new risks or sensitivity

4. Retention and Disposal of Information Assets

Retention and disposal are critical stages in the **information asset lifecycle**. Every information asset—whether digital or physical—must be **retained for a defined period** to meet **legal, operational, or business needs** and **disposed of securely** when no longer required.

Retention of Information Assets

✅ **Definition:**

Retention refers to the **period of time an organization preserves an information asset** in its usable form.

✅ **Purpose:**

- Meet **legal and regulatory requirements** (e.g., tax, financial records)
- Support **audits, investigations, or legal cases**
- Maintain **historical or operational relevance**

✅ **Factors Determining Retention:**

- Type and sensitivity of the asset
- Legal obligations (e.g., data protection laws, financial regulations)
- Business and operational needs
- Risks associated with early disposal or prolonged storage

✅ **Examples:**

- Employee records retained for 7 years after resignation
- Financial records retained for the duration mandated by tax laws

---

Disposal of Information Assets

✅ **Definition:**

Disposal is the **permanent and secure destruction or deletion** of an information asset once its retention period has ended.

✅ **Purpose:**

- Prevent unauthorized access or misuse
- Reduce storage costs and legal risks
- Maintain compliance with **data protection laws** (e.g., GDPR's "right to be forgotten")

✅ **Secure Disposal Methods:**

Type of Asset	Secure Disposal Method
Paper Documents	Shredding, incineration
Digital Media	Degaussing, physical destruction
Hard Drives/SSDs	Overwriting (multiple passes), crushing
CDs/USB Drives	Incineration, certified destruction vendors

Responsibilities:

- **Asset Owners**: Ensure assets are retained and disposed of according to policy
- **Custodians**: Implement secure deletion and maintain records of disposal
- **Users**: Follow retention/disposal rules and report any anomalies

5. Authorization for Access – Owner

- Asset owners have access to information based on **contractual obligations** and **sensitivity of the asset**.
- They handle access to proprietary software, trade secrets, and business-critical assets.
- Owners must ensure information is shared appropriately and protected according to legal, contractual, and organizational policies.

Example: A department head is responsible for controlling access to confidential financial reports under licensing or intellectual property terms.

---

6. Authorization for Access – Custodian

- Custodians are **responsible for the operational and technical protection** of information.
- They maintain the **accuracy and integrity** of sensitive or public information as directed by the owner.
- Typical tasks include backup, patching, antivirus configuration, and secure handling of devices.

Example: An IT staff member backs up customer data daily and ensures security patches are up to date.

---

7. Authorization for Access – User

- Users must **authenticate themselves** to access information using:
  - **Something they know** (e.g., password, PIN) – least secure, least costly
  - **Something they have** (e.g., access card) – more secure, more costly
  - **Something they are** (e.g., biometrics) – most secure, most costly
- Access is **granted based on "need to know"** and is limited to the job function.
- Users must follow all security policies and report any violations.

Example: An employee uses a fingerprint scanner and password to log in and access only their assigned department's files.

Unit 5 – Risk Analysis and Risk Management

---

1. Risk Management

Asked: Dec 2019, May 2023

- Risk Management is the **identification, assessment, prioritization**, and **control** of risks to reduce them to an acceptable level.
- It's essential to the **decision-making process**, security planning, and resource allocation.
- Aims to **preserve confidentiality, integrity, and availability** of information assets.

---

2. Risk Analysis Process

1. **Identify the Risk**
   → Create a risk register
2. **Analyze the Risk**
   → Determine **likelihood + consequence**

3. **Evaluate/Rank the Risk**
   → Acceptable or critical?
4. **Treat the Risk**
   → Risk response plan: mitigate/transfer/accept/avoid
5. **Monitor and Review**
   → Continuous tracking

---

3. Probability of Occurrence

Asked: Dec 2019, Dec 2022, May 2021

- Probability is the **likelihood** a risk will occur.
- Can range from **just above 0% to just below 100%**
- Tools: **Risk Probability-Impact matrix**, expert opinion, and historical data.
- Combined with impact to calculate **risk score**.

---

4. Impact of Threat in Information Security

Asked: May 2022, Dec 2022

- A threat **impacts** security when it leads to:
  - Data loss or theft
  - Service disruption (DoS, ransomware)
  - Financial or reputational loss
- Impact varies by **asset type**, **business criticality**, and **severity of exposure**

---

5. Types of Risk

Asked: Dec 2019

Type of Risk	Examples
Physical Damage	Fire, water, vandalism
Human Interaction	Accidental deletion, insider threat
Equipment Malfunction	Hardware failure, system crash
Attacks	Viruses, hacking, phishing
Data Misuse	Fraud, espionage, data theft
Application Errors	Buffer overflows, input validation failures

---

6. Risk Mitigation

Asked: July 2019, Dec 2021, May 2021, May 2022, Dec 2022

Mitigation = **Reducing the impact or likelihood** of risks.

Approaches include:

- Risk Assumption
- Risk Avoidance
- Risk Limitation (e.g., antivirus, patching)
- Risk Planning
- Research & Acknowledgment
- Risk Transference (e.g., insurance)

---

7. Risk Control Types/Categories

Asked: July 2019, May 2023

Control Type	Purpose
Preventive	Stops an incident before it occurs (e.g., firewall)
Detective	Identifies incidents after they happen (e.g., IDS)
Corrective	Restores systems to normal (e.g., backup restore)
Compensating	Alternate controls when main ones are unavailable
Deterrent	Discourages violations (e.g., legal warning)

---

8. Risk Control Strategies

- **Avoidance**: Eliminate the risk entirely
- **Mitigation**: Apply controls to reduce impact
- **Transference**: Shift risk (e.g., outsourcing, insurance)
- **Acceptance**: Acknowledge and accept the risk if cost of control > risk impact

---

9. Cost Analysis / Cost-Benefit Analysis (CBA)

Asked: Dec 2020, May 2021, Dec 2022, May 2022

A **CBA** compares the **costs of security controls** vs **expected benefits** (risk reduction, compliance, recovery).

Steps:

1. Define goals
2. Identify stakeholders (primary, secondary)
3. Measure cost & benefit
4. Predict outcomes
5. Convert into a common unit (e.g., currency)
6. Discount rate
7. Calculate **Net Present Value**
8. Perform sensitivity analysis
9. Choose best option

---

10 Ways to Mitigate Information Risk

Asked: Dec 2019

1. Use firewalls and intrusion prevention systems
2. Regular patching and updates
3. Employee awareness training
4. Implement access controls
5. Data encryption
6. Backup and disaster recovery plans
7. Secure software development practices
8. Physical security controls
9. Incident response plan
10. Periodic risk assessments

Unit 6 Access Control

2-MARK QUESTIONS

Term	Definition
User Identity	Part of Identity and Access Management (IAM); uniquely identifies individuals or systems, controlling resource access.
Network	A system of interconnected computers and devices; NAC restricts access based on endpoint compliance.
Event Logging	Records and stores key events (errors, warnings, successes) from software or hardware into logs for later review.
Cryptography	Technique to encode data securely using symmetric/asymmetric encryption or hash functions.

Term	Definition
Unauthorized Access	When a person or system accesses data or resources without proper authorization.
Privilege Management	Managing elevated access to systems using Privileged Access Management (PAM) tools.
Logs	Data generated and stored during system activity—includes date/time, source, event ID, etc..
Decryption	The process of converting encrypted (ciphertext) data back to its original (plaintext) form using a key.
Access Management	Defines how users are authorized post-authentication using policies and permissions.
Threat Identification	Process of spotting potential sources of harm to information systems.
Registries	Databases that store configuration settings and system preferences.
Encryption	Converts plaintext into unreadable ciphertext to prevent unauthorized access.

6-MARK QUESTIONS (Focused Explanations)

1. **Privilege Management**
    - Controls who can access what and at what level (Admin, User, etc.)
    - PAM enforces least privilege, manages passwords securely via vaults, and records session activities.
2. **Monitoring System Access Control**
    - Includes CCTV, logs, IDS/IPS.
    - Used to detect, alert, and prevent unauthorized access.
3. **Access & Privilege Management**
    - Defines both identity and access rights.
    - PAM implementation: policy, role assignment, tool provisioning.
4. **OS Access Control**
    - Grants login/logout and command-level access (Admin/User/MntSurv, etc.) using user-privilege mapping.
5. **Intrusion Detection System (IDS)**
    - Monitors traffic for known/unknown attack patterns.
    - Types: NIDS, NNIDS, HIDS.
6. **Network Access Control (NAC)**
    - Restricts access to networks based on device compliance (e.g., antivirus, updates).
7. **Event Logging**
    - Captures types (Info, Error, Audit), sources, and user logs for incident tracking and forensic analysis.

10-MARK QUESTIONS (Full Concepts)

1. **Intrusion Detection System in Detail**
    - Signature-based vs Anomaly-based
    - Types: NIDS, HIDS, NNIDS
    - Alerts, logging, and prevention strategies.
2. **Cryptography – Encryption and Decryption**
    - Symmetric (SKC), Asymmetric (PKC), Hashing
    - Use cases: data protection, integrity, authentication.
3. **Monitoring System Access Control**
    - Implementation of CCTV, IDS, logging
    - Security alerts, policy enforcement, audit trails.
4. **OS Access Control**
    - Privileges (Admin, Prov, User)
    - Access lifecycle (login, session control, logout).
5. **User Identity and Access Management (IAM)**
    - Covers creation, login, services, federation
    - Ensures “right access at right time” using policies.

UNIT 7: PHYSICAL SECURITY

2-MARK QUESTIONS

Term	Definition
Safe Disposal	Secure elimination of physical devices (e.g., shredding hard drives, wiping storage) to prevent data leaks.
Physical Security	Security measures to protect facilities, personnel, and hardware from physical harm.
Fire Prevention	Preventive measures like safe storage, fire-rated rooms, smoke detectors.
Fire Precautions	Protocols for evacuation, suppression, and smoke detection.
Fire Detection	Devices include: heat detectors, smoke detectors, flame detectors, gas sensors.

Term	Definition
Physical Assets	Tangible devices such as servers, laptops, printers, etc., which store or process sensitive data.

6-MARK QUESTIONS

1. **Asset Identification**
    - Identifies critical hardware/information for security priority
    - Helps with redundancy, backups, disaster recovery.
2. **Perimeter Security**
    - Involves IDS, CCTV, firewalls, DMZ, guards, barriers
    - Acts as first layer of defense.
3. **Safe Disposal of Physical Assets**
    - Shredding, recycling, third-party secure wipe services
    - Includes tracking inventory for disposal.
4. **Physical Security**
    - Layered approach using locks, guards, surveillance, access control.
5. **Business Requirements for Security**
    - Identify data dependencies, operation continuity, risk exposure tolerance.

10-MARK QUESTIONS

1. **Network Access Control**
    - Defines rules for endpoint devices before allowing network access
    - Supports compliance checks, user authentication.
2. **Steps in Safe Disposal of Assets**
    - Wipe → Decommission → Recycle or destroy
    - Includes data retention check and audit log.
3. **Identification of Critical Assets**
    - Based on business impact and security priority
    - May involve server duplication, critical file backups.
4. **Fire Prevention in IT Firms**
    - Use fireproof cabinets, smoke sensors, split power rooms
    - Daily checks, fire exits, waterless suppression systems.
5. **Perimeter Security (12 points)**
    - Border routers, VPNs, IDS, cameras, sensors, smart locks, walls, access zones, alarms, mantraps, biometric gates.