Information Security Basics:

Communities of Interest:

Managers and professional from information security (Protect IT Assets)
Managers and professional from field of IT (Support Business Objectives)
Managers and professional from rest (Articulate Policies and allocate resources)

Security - Quality of being secured from danger

Areas of Security - Physical, Operational, Communication, Cyber, Network

Components of Security:
Computer Security - Confidentiality (Identity - Preserve Self)
Data Security - Integrity (Time - Preserve Self over time)
Network security - Network (Cycles - Preserve Self as part of cycles)

The Committee on National Security Systems (CNSS) McNumber Cube

Confidentiality | Integrity | Availability
Storage | Process | Transformation
Policy | Education | Technology

Weakness - Do not control , Single Perspective

Confidentiality: ensures that only those with sufficient privileges may access certain information (Our sense of self is preserved with only we allow)

Integrity: The quality or state of being whole, complete, and uncorrupted.(Our sense of self is preserved if memory/time is preserved)

Availability: The characteristic of information that enables user access to information in a required format, without interference or obstruction (The self moves in cycles, availability allow destruction for new self to come in existence)

Privacy (Honoring other Confidentiality to be used their data for purpose allowed)

Requirement for preserver

Identification (I see), Authentication (I ask), Authorization (I allow or deny), Accountability (I recall)

Accountability do not violate privacy is it matter of recall, it only become issue what is done with that memory

Manager - Mind (Collect, Interact, Decide)
Leader - Self (Purpose, Direct, Motivate)

InfoSec Management:

Management (Mind)

POLC (Plan, Organize, Lead, Control)

Planning - Strategic (long term) Tactical (short term) Operational (Day to Day)
Goals - (End Result of Planning) Objective - (Intermediate Point of Planning)

Organizing (How? By Whom? What? By When? What is needed?) - Structure, HR

Leading (Direction ,Motivation, Behaviour)

Controlling (Standards, Measurement, Comparison, Action)

Solving Problems
Recognize and define the problem, Gather facts and make assumptions, Develop possible solutions, Analyze and compare possible solutions , Select implement and evaluate a solution

The six P's
➢ Planning : Goals and Objectives
➢ Policy : Guidelines (Enterprise information security policy (EISP) > Issue-specific security policy (ISSP) > System-specific policies (SysSPs))
➢ Programs (operations that are specifically managed as separate entities, habits)
➢ Protection (risk assessment and control, protection mechanisms, technologies, and tools)
➢ People
➢ Projects (To achieve various objectives)

PMBoK (Project Management Body of Knowledge)
Integration, Scope, Time , Cost, Quality, HR, Communication, Risk, Procurement

Projectitis ➢ Occurs when the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than accomplishing meaningful project work • Precursor to projectitis ➢ Developing an overly elegant, microscopically detailed plan before gaining consensus for the work required

WBS
Task Sequencing
(PERT) (Difficult to maintain for large)
Critical path - slowest path
Activity (earliest start, earliest finish)/ Duration (latest start, latest finish)
Gantt

Precursor to planning
Value (Principle), Vision(Want), Mission (Reason for want = purpose and scope.)

Planning for Security & Contingencies:

- It's a top-down process, initiated by leadership and tailored through the organization's structure. (CEO > CIO > CISO)

Strategic to Operational Planning
Strategic Planning: High-level, long-term goals (SMART (Specific, Measurable, Attainable, Relevant, Timebound) objectives).
Tactical Planning: Mid-range goals; bridges strategy and operations.
Operational Planning: Day-to-day functions and resource coordination.

Strategic planning and corporate responsibility are accomplished by using governance, risk management, and compliance (GRC).
GRC creates the environment in which planning can safely occur.

IDEAL model by the Corporate Governance Task Force (CGTF)

Initiating – Establish commitment, define objectives, and secure resources to launch the governance improvement effort.

Diagnosing – Assess current governance practices to identify strengths, weaknesses, and gaps.

Establishing – Develop a strategic plan outlining clear goals, roles, and processes for improvement.

Acting – Implement the planned governance initiatives and monitor progress.

Learning – Evaluate results, capture lessons learned, and adapt for ongoing improvement.

SecSDLC (Security Systems Development Life Cycle)
Investigation – Define goals, scope, feasibility.
Analysis – Review current controls, risks.
Design – Logical & physical planning, controls, policies.
Implementation – Deploy solutions, train staff.
Maintenance & Change – Monitor, update, improve.

Attack: A deliberate act that exploits a vulnerability to achieve the compromise of a controlled system
Vulnerability: An identified weakness of a controlled system in which necessary controls that are not present or are no longer effective
Exploit: A technique or mechanism used to compromise a system

Design (NIST, ISO, SETA (Security Education, Training, Awareness))

Controls
- Managerial – Policy and oversight.
- Operational – Day-to-day safeguards. (Disaster recovery • Incident response planning • Personnel security • Physical security • Protection of production inputs and outputs)
- Technical – System-level protections.

Core Components of Contingency Planning
- Business Impact Analysis (BIA): This preparatory step identifies critical systems and functions, evaluates potential attack scenarios, and assesses associated damage.
- Incident Response Planning (IRP): Focused on immediate actions during an incident, it sets up a dedicated team (often in the form of a Computer Security Incident Response Team or CSIRT) to detect, evaluate, and respond to security breaches.
- Disaster Recovery Planning (DRP): This plan outlines the steps to restore operations at the primary site after catastrophic events, distinguishing between natural and man-made disasters.
- Business Continuity Planning (BCP): Aimed at maintaining essential functions, this plan establishes alternative operational sites (e.g., hot, warm, or cold sites) until normal operations can resume.

3. Development and Management Process
The contingency planning process follows a structured sequence:
- Formulate a policy statement that grants authority and outlines the planning framework.
- Conduct the BIA to prioritize critical systems.
- Develop recovery strategies along with preventive controls to mitigate risks.
- Create detailed IT contingency plans, including protocols for detecting and addressing incidents.
- Regularly test, train, and update the plans to ensure their efficacy over time.

4. Team Roles and Responsibilities
Four distinct teams play pivotal roles:
- The Contingency Planning Management Team (CPMT) oversees the entire process, gathering key system and threat information.
- The Incident Response Team specifically handles immediate responses to detected incidents.
- The Disaster Recovery Team focuses on re-establishing operations at the primary site after major disruptions.
- The Business Continuity Team is responsible for establishing and maintaining operations at alternate sites as needed.

5. Operational Procedures During Incidents

Detailed procedures cover preparation (establishing roles and backup strategies), real-time actions (notification, containment, and documentation), and post-incident recovery (damage assessments, evidence collection, repair, and review). Continuous evaluation and refinement (through after-action reviews) are essential to improving future responses.

6. Testing and Continuous Improvement

Regular testing of plans using various methods (desk checks, structured walkthroughs, simulations, parallel testing, and full interruption tests) helps identify gaps and drive continuous process improvement. Keeping the plans updated ensures that organizations are prepared for evolving threats and can confidently restore business operations after an incident.

Policies & Program Development:

policies are managerial directives that outline acceptable behaviors and standards for system usage.

Foundation of an InfoSec Program, Management Tone and Accountability, Cost-Effective Control

The Bull's-Eye Model is presented as a systematic approach with four layers:

- Policies: The outer layer, setting the overall guidelines.
- Networks: The first environment where threats encounter the organization.
- Systems: The hardware, software, and other IT components.
- Applications: The specific application services that processes data

Enterprise Information Security Policy (EISP): A high-level policy outlining the organization's security philosophy, strategic direction, and framework.It aligns closely with the organization's vision and mission.

Issue-Specific Security Policies (ISSP): These are detailed policies targeting specific issues or technologies. They articulate both the allowed and prohibited uses of organizational resources, include guidelines for management, protect the company from legal liabilities stemming from misuse.

System-Specific Security Policies (SysSP): Focused on systems configuration and operation, these policies are often technical in nature. They can be divided into:

- Managerial Guidance: Outlining management intent for technology usage.
- Technical Specifications: Providing detailed instructions such as access control rules, configuration settings, and system administration practices.

Key Components: Purpose and Need, Defined Roles and Responsibilities, Standards and Guidelines, Enforcement and Penalties,Review and Revision Processes:

Policy Lifecycle: Development,Dissemination,ReviewComprehension: Verifying Compliance: Securing employee agreement,Uniform Enforcement: Applying policies consistently across the organization.

Security Models & Practices:

SETA (Security Education, Training, and Awareness):
Improves employee security behavior through education, hands-on training, and awareness. Training is role-specific (user, manager, technical) and delivered in multiple formats.

Security Program Fundamentals:
Covers InfoSec program structure, roles, and integration of SETA. Focus on proper organization and placement within the company.

InfoSec Models & Frameworks:
Blueprints describe current and required controls; frameworks provide structure to develop blueprints; security models offer reusable templates based on best practices.

Access Control Models:
Manage access via identification, authentication, authorization, accountability. Principles include least privilege, need-to-know, and separation of duties. Control types: preventative, detective, corrective, etc. Categorized as management (strategic), operational (process), and technical (tactical). Access models:

- MAC: Centralized, strict classification-based
- DAC: User-controlled, flexible
- Nondiscretionary: Role/task-based, hybrid approach

Data Classification & Personnel Security:
Military (5-level) and simplified classification systems, with periodic review and proper labeling. Personnel access based on clearance and need-to-know; includes policies for asset handling and clean desk practices.

Advanced Access Control & Architecture:
Lattice-based access uses matrices for clearance-based access. Key models: Trusted Computing Base (TCB), Reference Monitor, and covert channels (hidden data flows).

Security Evaluation Standards:

- TCSEC (Orange Book): US system security standards
- ITSEC & Common Criteria: International standards
- Models: Bell-LaPadula (confidentiality), Biba (integrity), Clark-Wilson (commercial control), Brewer-Nash (conflict of interest)

Security Management Models:

- ISO 27000 Series: Framework for implementing and improving ISMS
- NIST SP 800 Series: Comprehensive guidance for risk, planning, and incident handling
- COBIT: Governance through detailed controls
- COSO: Internal controls for fraud prevention

NIST Framework Highlights:
Covers everything from basics to advanced security. Emphasizes continuous risk management and integration with operations. Offers templates, control families, and practical guidance.

MAC vs DAC Comparison:
MAC offers high security with low flexibility, suitable for high-sensitivity data. DAC is user-friendly and flexible but less secure. Nondiscretionary models (RBAC) offer a balanced middle ground.

Security Management Practices:
Benchmarking (due care/diligence, best practices) and baselining (trackable metrics) help assess and improve performance.

InfoSec Performance Measurement:
Use quantifiable, repeatable metrics to assess effectiveness. Categories: policy execution, service delivery, incident impact. Requires strong management support and continuous monitoring.

Identifying Information Assets:

    - Assets include people, data, procedures, hardware, software, and networking components.
    - Managers should compile a comprehensive asset inventory.
- Assigning Value:
    - Once assets are identified, a relative value must be assigned to each by comparing critical factors such as revenue generation, replacement cost, and overall importance to organizational success.
- Knowing the Enemy:
    - This involves a detailed assessment of the threats facing the organization. Only applicable threats are retained after eliminating those that are irrelevant.
    - A threat assessment involves questions about the likelihood of occurrence, success probability, potential losses, and the organization's preparedness.A specialized tool, the Threats-Vulnerabilities-Assets (TVA)

Protection Mechanisms: Fundamentals of access control, evolution of firewalls, IDPS types and detection methods, and key cryptographic principles (symmetric vs. asymmetric, PKI, digital certificates).
Personnel, Laws & Ethics: Staffing, professional credentials, employment policies, and differences between laws, policies, and ethics.

Structuring the InfoSec Program: The program's structure depends on variables like organizational culture, size, and budgets (personnel and capital). As organizations grow, even though the infrastructure becomes more complex, spending per user typically declines.

Functional Components of InfoSec: Essential functions include risk assessment and management, systems testing, policy making, legal assessments, incident response, compliance, centralized authentication, and network and systems security administration. The slide further categorizes roles in InfoSec into those that define policy, those who build technical solutions, and those who administer security operations.

Risk Assessment and Quantification

$$R = (L_v \times I) \times (1 - R_c + U)$$

where

- R is the **risk** rating factor;
- L_v is the **likelihood** of vulnerability occurrence;
- I is the **impact value** of the information asset;
- R_c is the percentage of risk mitigated by **current controls**;
- U is the **uncertainty** of current knowledge of the vulnerability.

Identifying and Documenting Controls

Once the risks have been thoroughly assessed, the next step is to brainstorm possible controls to mitigate the residual risk (risk remaining after current controls are considered). Controls are generally categorized into:

- Policies: Guidelines and procedures that govern secure behavior.
- Programs: Ongoing initiatives, including training and awareness.
- Technical Controls: Specific technological measures, such as firewalls, encryption, or intrusion detection systems.

In addition to listing potential controls, all findings from the risk management process should be documented. A final deliverable is a comprehensive, ranked vulnerability risk worksheet that details:

- The asset inventory,
- Prioritized threats,
- Vulnerability findings, and
- The identified control options.

Risk Control Strategies

1. Defense Transference Mitigation Acceptance Termination

a. NIST SP 800-12, Rev. 1 — *An Introduction to Information Security*

- **Purpose**: Serves as a foundational primer for information security within federal systems.
- **Resources Provided**: Offers broad overviews of security principles, best practices, and high-level guidance for initiating, developing, and managing security programs.

b. NIST SP 800-14 — *Generally Accepted Principles and Practices for Securing Information Technology Systems*

- **Purpose**: Establishes principles and recommended practices that are considered essential for building secure IT systems.
- **Resources Provided**: Provides a framework of key security principles, functional practices, and implementation techniques to support effective security programs.

c. NIST SP 800-18, Rev. 1 — *Guide for Developing Security Plans for Federal Information Systems*

- **Purpose**: Guides organizations through the creation of security plans tailored to specific information systems.
- **Resources Provided**: Includes templates and instructions for detailing system boundaries, roles and responsibilities, and security control implementation.

d. NIST SP 800-30, Rev. 1 — *Guide for Conducting Risk Assessments*

- **Purpose**: Supports organizations in performing thorough risk assessments as part of a broader risk management program.
- **Resources Provided**: Offers structured methodologies for identifying threats, vulnerabilities, and likelihoods, and evaluating their impact on system security.

Risk Metrics and Control Cycle

- Risk Appetite & Residual Risk:
    - Risk Appetite: Represents the level of risk an organization is willing to accept balanced against usability; it is essentially a set of trade-offs between perfect security and functionality.
    - Residual Risk: Even after full implementation of risk controls, there is often a remaining (or residual) risk that must be aligned with the organization's risk tolerance.
- Risk Control Cycle: Once a particular control is selected and implemented, it must be continuously monitored for effectiveness. In essence, the process is cyclic—control implementation, measurement, and reassessment—to ensure that residual risk stays within acceptable bounds.

Cost-Benefit Analysis (CBA) and Asset Valuation

- Economic feasibility, cost, benefit, assess valuation, potential loss
- Assess value (AV), Exposure factor (EF), Annualized loss expectancy (ALE), single loss expectancy (SLE), annualized rate of occurrence (ARO),
- **SLE = asset value (AV) x exposure factor (EF)**
- **ALE = SLE * ARO**
- **CBA = ALE(prior) – ALE(post) – ACS**

Feasibility Analysis and Alternative Methodologies

To ensure the chosen risk control strategy is viable, various feasibility analyses are discussed:

- Feasibility Analysis Types:
    - Organizational Feasibility,Operational Feasibility,Technical Feasibility,Political Feasibility
    - Alternative Approaches and Frameworks: The lecture briefly introduces multiple risk management methodologies and frameworks beyond the basic risk control strategies:
    - OCTAVE: A methodology from CERT for balancing information asset protection with control costs.
    - Microsoft's Risk Management Approach: Integrates risk management with overall governance.
    - ISO Standards: For example, ISO 27005 and ISO 31000 provide robust frameworks for managing a broad array of risks.
    - NIST Risk Management Framework (RMF): Outlines guidelines (SP 800-39 and SP 800-37) to embed risk management into daily operations.
    - FAIR, Mitre, ENISA, and New Zealand's IsecT Ltd.: Additional frameworks and methodologies that offer alternative perspectives and methods for evaluating and managing risk.

- Packet Filtering Firewalls: The first generation, examining packet headers and filtering based on established rules (e.g., by IP, port, or protocol).
- Application-Level Firewalls: These operate at the application layer and often complement packet filters. However, their specificity can also be a limitation.
- Stateful Inspection Firewalls: The next step in sophistication, these track the state of active network connections using state tables. If a packet does not match a known connection state, the firewall consults its access control list.
- Dynamic Packet Filtering Firewalls: Introduce logic that adapts rules based on past packets rather than evaluating each packet on its own merits.

Architectural Implementations:

- Packet Filtering Routers: Common in many organizations to provide basic protection by acting as the first line of defense.
- Screened Host Firewalls and Dual-Homed Host Firewalls: Here, dedicated firewall systems (often acting as bastion hosts) work in tandem with routers, sometimes using Network Address Translation (NAT) to secure internal IP addresses.
- Screened-Subnet Firewalls: These configurations employ multiple layers (external filtering, bastion hosts in a DMZ) to manage connections from untrusted networks into secure, internal segments.

Key Functions and Types:

- Host-Based and Network-Based IDPS:
    - Host-Based IDPS monitors individual computing components or servers.
    - Network-Based IDPS observes traffic across the network, looking for malicious patterns or anomalies.
- Detection Approaches:
    - Signature-Based: Compares network activity against a database of known attack patterns. These systems require frequent updates.
    - Anomaly-Based: Establishes a baseline of normal activity and flags deviations, which can help detect novel or unknown attacks but might generate false positives.

Operational Considerations:

- The system should be sensitive enough to detect true threats without overwhelming administrators with alerts. Proper configuration, including the use of monitoring agents and consolidated management servers, is crucial to effective alerting and response.

Wireless Network Protection

Wireless networks typically use the IEEE 802.11 standards, and their security footprint can be adjusted by managing the power output of the wireless access points.

- Concerns include ensuring that access is limited to within the intended coverage area to prevent unauthorized connections (e.g., through war driving or rogue access points).

Protocols:

- Wired Equivalent Privacy (WEP) was an early protocol offering basic protection but is compromised by inherent cryptological flaws.
- Wi-Fi Protected Access (WPA) and its successor WPA2 (with implementations based on the Advanced Encryption Standard) offer improved security and authentication. Emerging protocols like WPA3 are also mentioned as advancements in securing wireless communications.

Cryptography and Encryption

Fundamental Concepts:

- Cryptography is presented as a control mechanism that supports confidentiality (through encryption), integrity (via hashing), authentication, and non-repudiation (through digital signatures).
- Key Terms:
    - Algorithm, Cipher, Plaintext/Ciphertext, and Key are defined as the basic building blocks of encryption systems.
    - Cryptosystems and the reversible processes of enciphering (encryption) and deciphering (decryption) are also explained.

Types of Encryption:

- Symmetric Encryption:
    - Uses the same secret key for both encryption and decryption.
    - It is noted for its efficiency but presents challenges in key distribution.
    - Common algorithms include DES, 3DES, and AES.
- Asymmetric Encryption:
    - Utilizes a pair of keys (public and private) with a reciprocal process. A message encrypted with one key can only be decrypted with the other.
    - This is essential for digital signatures and forms the basis of public key infrastructures (PKIs).
    - Algorithms such as RSA and ElGamal are referenced.
    - The inherent challenge lies in the complexity, as the number of keys increases exponentially with more participants.

Digital Signatures and Certificates:

- Digital Signatures: Provide non-repudiation, ensuring that a message's origin can be verified.
- Digital Certificates and Certificate Authorities (CAs): Work together to authenticate that a public key belongs to the claimed owner and has not been tampered with.

Hybrid Systems:

- To leverage the strength of both symmetric and asymmetric systems, hybrid systems are used. One common method—the Diffie-Hellman key exchange—allows for the secure exchange of symmetric keys using asymmetric techniques. This provides efficient, secure communication while mitigating the weaknesses of each standalone approach.

Management of Cryptographic Controls: Losing keys, mismanaging certificate authorities, or using weak cryptographic protocols can render the system vulnerable. Attention to proper configuration, key storage, updates, and adherence to legal requirements is paramount.

- Integration and Layering: No single control is sufficient on its own. Effective security is achieved by integrating multiple layers—from technical controls like firewalls and IDPSs to policies, training, and procedures.

- Continuous Monitoring and Evaluation: Whether it's scrutinizing firewall rule sets or fine-tuning IDPS alerts to avoid false positives, ongoing evaluation and adjustment are necessary to adapt to evolving threats.
- Balancing Security and Performance: Especially in firewalls, there's an inherent tension between thorough security screening and network performance. Logical errors in configurations can lead to unintended access or degradation of service.
- Future Growth and Scalability: When deploying security measures, the design must accommodate anticipated future network expansions and technology advancements.

Personnel and Security

- Staffing and HR Integration: Maintaining a secure environment depends on structuring and staffing the InfoSec department with well-qualified, appropriately credentialed personnel. This includes embedding security-focused procedures across all HR activities such as hiring, training, promotion, and termination.
- Roles and Responsibilities: The slide details three main categories of InfoSec positions:
    - Definers: Establish policies, guidelines, and standards.
    - Builders: Technical experts who design and implement security solutions.
    - Administrators: Manage security tools and monitor systems.
- Key Positions:
    - Chief Information Security Officer (CISO): Typically the top InfoSec position, usually reporting to the CIO, requiring broad expertise in technology, planning, and policy.
    - Security Manager: Responsible for day-to-day operations of the InfoSec program, often expected to have certifications (e.g., CISSP) and experience in business operations.
    - Security Technicians: Entry-level technologists who implement, configure, and troubleshoot security solutions.

Professional Credentials and Certification Cost

- The slide emphasizes that many organizations use professional certifications (like CISSP, SSCP from (ISC)² and CISA, CISM from ISACA) to gauge proficiency in InfoSec.
- Certifications can be costly and often require several years of work experience along with exam preparation, which deters those looking to take the exam lightly.

Employment Policies, Hiring, and Termination Practices

- Hiring: Security considerations should be integral to the hiring process—from detailed job descriptions to
- Termination: When an employee leaves, strict procedures (such as disabling system access and recovering all organizational property) must be followed to prevent potential data misappropriation or security breaches.

Personnel Security Practices

- Internal Controls: Practices like separation of duties, job and task rotation, and mandatory vacations are critical to prevent individual misuse of information.
- Least Privilege Principle: Employees should only have access to the information necessary for their roles, reducing the risk of abuse.
- Protection of Personal Data: Organizations must legally safeguard sensitive data pertaining to employees and nonemployees alike.

Legal Framework: Information security laws like the Computer Fraud and Abuse Act, Computer Security Act, HIPAA, and others (both domestic and international) are highlighted as pillars of the legal environment that InfoSec professionals must navigate.

> Effective deterrence of unethical or illegal behavior involves three conditions—the fear of penalty, the likelihood of being caught, and the chance that a penalty will be administered.