CISSP Study Notes

## Chapter 1 – Security Governance Through Principles and Policies

**CIA Triad**

* **Confidentiality**: Sensitivity, discretion, criticality, concealment, secrecy, privacy, seclusion, isolation
* **Integrity**: Accuracy, truthfulness, validity, accountability, responsibility, completeness, comprehensiveness
* **Availability**: Usability, accessibility, timeliness

**AAA Framework**

* **Identification:** claiming identity when attempting to access an area.
  + Usernames, unique identifiers, biometrics, digital certificates
* **Authentication**: Credentials, multi-factor authentication (MFA), single sign-on (SSO), federation
* **Authorization**: Role-based access control (RBAC), mandatory access control (MAC), discretionary access control (DAC), principle of least privilege
* **Auditing**: Auditing is a recording a log of the event or activities related to the system/subject.
* **Accounting**: Logs, audit trails, non-repudiation, monitoring
* **DAD Triad** – Risk of overprotection, authenticity, nonrepudiation & AAA Services

**Security Governance:** Policies, procedures, accountability, oversight, risk management, compliance

**3rd Party Governance:** External entity oversight that may be mandated by law, regulation, industry standards, contractual obligations, or licensing requirements. Generally involves an outside investigator/auditor.

**Concept of Abstraction:** Layers, separation, simplification, modularization

**Security Boundaries:** Trust zones, network segments, air gaps, perimeter defense, internal vs. external access

**Security Alignment with Business:** Mission, objectives, goals, risk tolerance, business strategy integration

**Business Case** Cost-benefit analysis, risk reduction, ROI (return on investment), alignment with business objectives

**Documentation Review** Act of exchanging and reviewing standards, compliances, and exceptions.

**Security Management Planning** Strategic, tactical, operational, incident response, business continuity, disaster recovery

**Formalized Security Policy Structure** Comprehensive Policies, standards, guidelines, procedures, baselines

**Key Security Roles** CISO, senior management, system administrator, security analyst, auditor

**Due Diligence & Due Care** Legal requirements, liability, best practices, proactive measures, reasonable actions

**Threat Modeling**

* Attack vectors, assets, vulnerabilities, threat actors, mitigation strategies
* **VAST** (Visual, Agile, and Simple Threat modeling)
* **DREAD** (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)
* **PASTA** (Process for Attack Simulation and Threat Analysis)
* **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)

**Supply Chain Risk Management (SCRM)** Third-party risks, vendor assessment, supply chain visibility, continuity planning, contingency measures

## Chapter 2 -Personnel Security & Risk Management Concepts

**Hiring & Employee Lifecycle**

* **Implications of Hiring New Employees**: Vetting, background checks, onboarding risks, access provisioning
* **Onboarding & Offboarding**: Clear processes for granting and revoking access, account setup/removal, training/debriefing
* **Employee Transfer**: Reassessing access privileges during internal transfers
* **Proper Termination Process**: Immediate revocation of access, exit interviews, data protection
* **Mandatory Vacations**: Detection of fraud or irregularities, separation of duties
* **User Behavior Analytics (UBA)** / **User and Entity Behavior Analytics (UEBA)**: Monitoring anomalous behavior for insider threats

**Access Control & Oversight**

* **Principle of Least Privilege**: Grant only necessary access to perform job functions
* **Employee Oversight**: Continuous monitoring, audits, role reviews, access validation

**Risk Management Overview**

* **Define Overall Risk Management**: Process of identifying, evaluating, and mitigating risks
* **Risk Analysis**: Identification, assessment, and prioritization of risks based on potential impact
* **Evaluate Threats**: Identify and assess external and internal threats to assets
* **Terminology**: Asset, Asset Valuation, Threats, Threat Agent/Actors, Threat Events, Threat Vector, Vulnerability, Exposure, Risk, Safeguards, Attack, Breach & Hazard

**Risk Analysis Techniques**

* **Qualitative Risk Analysis**: Subjective assessment based on scenarios, likelihood, and impact
* **Quantitative Risk Analysis**: An objective numerical analysis based on statistical methods

**Risk Formulas**

* **Asset Value (AV)** = $
* **Exposure factor (EF)** = % Loss
* **Single Loss Expectancy (SLE)**
  + **Formula**: SLE = asset value (AV) \* exposure factor (EF)
* **Annualized rate of occurrence (ARO)** = # / year
* **Annualized Loss Expectancy (ALE)**
  + **Formula**: ALE = SLE \* annualized rate of occurrence (ARO)
* **Annual cost of the safeguard (ACS)** = $ / year
* **Safeguard Evaluation Formula**
  + **Formula**: (ALE1 (before safeguard) – ALE2 (after safeguard)) - annual cost of safeguard (ACS)
* **Qualitative vs Quantitative**
  + **Qualitative:** Estimations, Opinionated, less objective, may use cost/benefit analysis
  + **Quantitative:** Math Functions, Cost/Benefit Analysis, supports automation, high volume of info, time

**Risk Response & Control**

* **Options for Handling Risk**: Avoid, transfer/assign, mitigate/reduce, reject/ignore, acceptance
* **Security Control Assessment (SCA)**: Evaluating the effectiveness of implemented security controls
* **Security Monitoring & Measurements**: Ongoing risk tracking, metric analysis, incident detection
* **Risk Reporting**: Regular updates to stakeholders detailing current risk posture
* **Total Risk = Threat + Vulnerabilities + asset value**
* **Residual Risk = Total Risk – Controls gap**

**Risk Management Frameworks**

* **Cybersecurity Framework 2.0:** Identify, Protect, Detect, Respond, Recover & Govern
* **Risk Maturity Model (RMM)**: Levels of risk management maturity, from ad hoc to optimized practices
  + Prepare (central), {Categorize, Select, Implement, Assess, Authorize & Monitor}

**Legacy Systems & Risks**

* **Legacy System Security Risk**:
  + **End of Life (EoL)**: No more updates or patches available
  + **End of Service Life (EoSL)**: Vendor no longer supports the system
  + **End of Support (EoS)**: No security updates, increasing vulnerabilities

**Human Factors in Security**

* **Social Engineering**: Exploiting human psychology to gain unauthorized access (e.g., phishing)
  + **Principles:** Authority, Intimidation, Consensus, Scarcity, Familiarity, Trust & Urgency
  + **Tactics:** Eliciting Information, Prepending, Phishing, Smishing, Vishing, Spear Phishing, Whaling, Spam, Shoulder Surfing, Invoice Scams, Hoax, Impersonation & Masquerading, Tailgating & Piggybacking, Baiting, Dumpster Diving, Identity Fraud, Typo squatting, Influence Campaigns, Hybrid Warfare, Social Media
* **Security Awareness Training & Education**: Regular training on security best practices, evolving threats
* **Periodic Content Reviews & Effectiveness Evaluations**: Assess and update training content to ensure relevance

## Chapter 3 Business Continuity Planning

**Disaster Recovery Planning (DRP)**

**Business Continuity Planning (BCP) Process**

* **Four Steps of BCP Process**:
  1. **Project Scope & Planning**
  2. **Business Impact Analysis (BIA)**
  3. **Continuity Strategy Development**
  4. **Plan Approval & Implementation**

**BCP Lifecycle – BCP Development, BCP Testing, Training & Maintenance, BCP Implementation**

**BCP Team & Analysis**

* **Perform Business Organization Analysis**: Understand the structure, mission-critical functions, and interdependencies within the organization
* **Necessary Members of BCP Team**: Senior management, IT, legal, HR, operations, risk management, and key business unit leaders

**Legal & Regulatory Requirements**

* **Legal & Regulatory Requirements of BCP**: Compliance with laws, industry standards, and contractual obligations, including data protection laws (e.g., GDPR, HIPAA)

**Business Impact Analysis (BIA)**

* **Stages of Business Impact Analysis (BIA) Process**:
  1. **Identify Priorities**
  2. **Risk identification**
  3. **Likelihood assessment**
  4. **Impact Analysis**
  5. **Resource prioritization**

**Continuity Strategy Development**

* **Process Used to Develop a Continuity Strategy**: Identify recovery options, establish alternative processes, and implement redundancy measures (e.g., backup sites, cloud services)

**BCP Documentation**

* **Importance of Comprehensive Documentation Around BCP**: Detailed documentation of procedures, roles, communication plans, and recovery processes; ensures clarity during emergencies

## Chapter 4 - Laws, Regulations, & Compliance

**Legal Systems & Cyber Law**

* **Difference Between Criminal, Civil, and Administrative Law**:
  + **Criminal Law**: Punishes offenses against society, prosecuted by the government
  + **Civil Law**: Resolves disputes between individuals or organizations, often involves compensation
  + **Administrative Law**: Governs regulatory agency rules and compliance, impacting businesses

**Cybercrime & Major Laws**

* **Major Cybercrime Laws**:
  + **Computer Fraud and Abuse Act (CFAA)**: Criminalizes unauthorized computer access
  + **Electronic Communications Privacy Act (ECPA)**: Protects electronic communications from unauthorized access and wiretapping

**Intellectual Property & Licensing**

* **Difference Between Copyright, Trademarks, Patents, and Trade Secrets**:
  + **Copyright**: Protects original works of authorship (e.g., software code, music)
  + **Trademarks**: Protects brand names, logos, and symbols
  + **Patents**: Protects inventions and processes
  + **Trade Secrets**: Protects confidential business information (e.g., formulas, methods)
* **Digital Millennium Copyright Act (DMCA)**: Protects copyrighted digital content and criminalizes circumvention of copyright protections
* **Economic Espionage Act**: Criminalizes theft or misappropriation of trade secrets, especially for economic advantage

**Software Licensing & Agreements**

* **Types of License Agreements**: Proprietary licenses, open-source licenses, End User License Agreement (EULA)
* **Software License Agreements**: Define terms for using, distributing, and modifying software

**Data Breach Notification**

* **Notification Requirements**:
  + **California SB 1386**: Requires notification of data breaches involving personal information
  + **HIPAA**: Mandates breach notification if protected health information (PHI) is compromised
  + **GDPR**: Strict notification rules for personal data breaches within 72 hours of discovery

**International Privacy Laws**

* **General Data Protection Regulation (GDPR - EU)**: Comprehensive privacy law governing data protection and privacy in the European Union
* **Personal Information Protection and Electronic Documents Act (PIPEDA - Canada)**: Governs the collection, use, and disclosure of personal information
* **Personal Information Protection Law (PIPL - China)**: Regulates personal data handling within China
* **Protection of Personal Information Act (POPIA - South Africa)**: Governs the processing of personal information to protect privacy

**Compliance & Security Integration**

* **Importance of a Well-Rounded Compliance Program**: Addresses regulatory requirements, internal policies, and continuous improvement
* **Incorporate Security into Procurement & Vendor Governance**: Evaluating vendor security practices, including contract requirements and risk assessments
* **Compliance & Information Protection**: Identifying applicable laws, industry standards, and regulatory mandates
* **Legal & Regulatory Issues Pertaining to Security**: Understanding the impact of legal frameworks on security policies, risk management, and incident response

**Key Laws Overview**

* **Computer Fraud and Abuse Act (CFAA)**: Criminalizes unauthorized computer access
* **Electronic Communications Privacy Act (ECPA)**: Protects against electronic surveillance and unauthorized access
* **Copyright, Trademarks, Patents & Trade Secrets**: Protect intellectual property
* **Software License Agreements**: EULA, proprietary vs. open-source
* **California SB 1386 & GDPR Equivalents**: Mandates data breach notifications across US states and internationally

## Chapter 5 – Protecting the Security of Assets

**Data & Asset Classification**

* **Importance of Data & Asset Classification**: Establishes data categories by sensitivity and criticality (e.g., public, confidential, restricted) to apply appropriate security measures and regulatory compliance

**Sensitive Information Types**

* **PII (Personally Identifiable Information)**: Information that can identify an individual (e.g., name, SSN, email)
* **PHI (Protected Health Information)**: Health-related data protected under healthcare regulations (e.g., HIPAA)

**Managing Sensitive Information**

* Access restrictions, encryption, data masking, secure storage, least privilege

**Data States**

* **Three Data States**:
  + **Data at Rest**: Stored data, often requiring encryption and physical protection
  + **Data in Transit**: Data in motion, needing secure transmission protocols (e.g., TLS)
  + **Data in Use**: Actively processed data, protected through secure access and memory protection

**Data Loss Prevention (DLP)**

* Tools and processes to detect, monitor, and prevent unauthorized data access, sharing, or leakage

**Data Destruction & Data Remanence**

* **Data Destruction Methods**: Shredding, degaussing, incineration, cryptographic erasure
* **Data Remanence**: Residual data after deletion, requiring secure wiping to prevent recovery

**Record Retention Policies**

* Defines retention timelines, ensuring legal and regulatory compliance for data storage and deletion

**End of Life (EoL) vs End of Support (EoS)**

* **End of Life (EoL)**: No new updates or support provided
* **End of Support (EoS)**: Manufacturer ends security updates, increasing vulnerability risk

**Digital Rights Management (DRM)**

* Controls access and usage of digital content, protecting intellectual property and sensitive information

**Cloud Access Security Broker (CASB)**

* Enforces security policies across cloud services, enhancing visibility and control over data in cloud applications

**Data Anonymization Techniques**

* **Pseudonymization**: Replaces identifying data with pseudo identifiers, allowing data linkage under certain conditions
* **Tokenization**: Replaces sensitive data with non-sensitive tokens, typically reversible through a secure lookup table
* **Anonymization**: Irreversible data transformation, removing identifiable elements to protect privacy

**Responsibilities for Data Roles**

* **Data Owner**: Defines data sensitivity, access levels, and retention requirements
* **Data Custodian**: Manages data storage, backups, and protection controls
* **Data User**: Accesses and uses data according to policy

**Security Control Baseline**

* Standardized set of security controls applied across the organization, ensuring foundational security measures are met

## Chapter 6 – Cryptography

**Cryptosystem Fundamentals**

* **Role of Confidentiality, Integrity & Nonrepudiation in Cryptosystems**:
  + **Confidentiality**: Protects data from unauthorized access
  + **Integrity**: Ensures data has not been tampered with
  + **Nonrepudiation**: Prevents denial of actions or data transactions, often achieved through digital signatures

**Authentication & Cryptosystems**

* **How Cryptosystems Achieve Authentication**:
  + Use of **digital certificates**, **hash functions**, and **public key infrastructure (PKI)** to verify identity

**Cryptography Terminology**

* **Plaintext**: Original readable data
* **Ciphertext**: Encrypted, unreadable data
* **Key**: Secret value used in the encryption and decryption process
* **Algorithm**: Mathematical formula for encryption and decryption

**Codes vs. Ciphers**

* **Code**: Substitutes words or phrases (e.g., "Sky King" for an operation)
* **Cipher**: Transforms individual characters or bits of data
  + **Types of Ciphers**: Substitution, transposition, stream, and block ciphers

**One-Time Pad Requirements**

* **Requirements**: Truly random key, key as long as the message, key used only once, and secure key distribution

**Key Concepts**

* **Split Knowledge**: Dividing a key or secret among multiple individuals to prevent any single person from having full knowledge
* **Work Function**: Measurement of the time and effort needed to break a cryptosystem; increasing complexity improves security

**Key Security Importance**

* **Importance of Key Security**: Protecting encryption keys is crucial for maintaining the security of the system
  + **Modern Standards**: Keys should be at least 128 bits in length

**Symmetric vs. Asymmetric Cryptosystems**

* **Symmetric Cryptography**: Uses a single key for both encryption and decryption (e.g., AES)
* **Asymmetric Cryptography**: Uses a pair of keys (public and private) for encryption and decryption (e.g., RSA)

**Operational Modes of Symmetric Cryptosystems**

* **Electronic Codebook (ECB)**: Simplest mode, less secure, identical blocks yield identical ciphertext
* **Cipher Block Chaining (CBC)**: Each block of plaintext is XORed with the previous ciphertext block
* **Cipher Feedback (CFB)**: Converts a block cipher into a stream cipher
* **Output Feedback (OFB)**: Similar to CFB but pre-processes the keystream
* **Counter (CTR)**: Uses a counter value for each block, enabling parallel processing
* **Galois/Counter Mode (GCM)**: Provides confidentiality and integrity
* **Counter with Cipher Block Chaining-Message Authentication Code (CCM)**: Combines CTR mode for confidentiality and CBC-MAC for authentication

**Advanced Encryption Standard (AES)**

* **AES**: A widely used symmetric encryption standard
  + **Key Lengths**: 128-bit, 192-bit, and 256-bit keys for varying levels of security

## Chapter 7 – PKI and Cryptographic Applications

**Asymmetric Cryptography Key Types**

* **Public Key**: Used for encryption and verifying digital signatures
* **Private Key**: Used for decryption and creating digital signatures
* **Session Key**: Symmetric key exchanged using asymmetric encryption, used for a single session

**Major Public Key Cryptography Types**

* **RSA**: Commonly used for secure data transmission and digital signatures
* **Elliptic Curve Cryptography (ECC)**: Provides strong security with shorter keys and lower computational requirements
* **Diffie-Hellman**: Primarily used for secure key exchange over public networks

**Hash Functions**

* **Fundamental Requirements**: Deterministic, efficient, preimage resistant, and collision resistant
* **Major Hashing Algorithms**: SHA-256, SHA-512 (part of the SHA-2 family); MD5 (deprecated due to collision vulnerabilities)

**Cryptographic Salt**

* **Purpose**: Adds random data to passwords before hashing to prevent attacks using precomputed hash tables (e.g., rainbow tables)

**Digital Signatures**

* **Generation**: Created using a private key to ensure the data's authenticity and integrity
* **Verification**: Validated using the corresponding public key

**Public Key Infrastructure (PKI)**

* **Definition**: Framework managing public key encryption and digital certificates
* **Components**: Certificate Authority (CA), Registration Authority (RA), digital certificates, certificate revocation lists (CRL)

**Applications of Cryptography**

* **Secure Email**:
  + **Protocols**: S/MIME (Secure/Multipurpose Internet Mail Extensions), PGP (Pretty Good Privacy)
* **Secure Web Activity**:
  + **Protocols**: HTTPS, SSL/TLS
* **Secure Networking**:
  + **Protocols**: VPNs, SSL/TLS, IPSec

**IPSec (Internet Protocol Security)**

* **Purpose**: Provides security for IP communications through authentication and encryption
* **Components**:
  + **Authentication Header (AH)**: Ensures data integrity and authenticity
  + **Encapsulating Security Payload (ESP)**: Ensures data confidentiality, integrity, and authentication

**Common Cryptography Attacks**

* **Brute Force**: Systematically guessing all possible key values
* **Dictionary Attack**: Using a list of probable passwords to guess the correct one
* **Rainbow Table Attack**: Cracking hashed passwords using precomputed hash tables
* **Man-in-the-Middle (MitM)**: Intercepting and possibly altering communication between parties
* **Replay Attack**: Re-sending captured data packets to mimic legitimate requests
* **Birthday Attack**: Leveraging hash function collisions to compromise data integrity

## Chapter 8 –Principles of Security Models, Designs, and Capabilities

**System Types**

* **Open Systems**: Interoperable with different devices and platforms, but may have increased vulnerability
* **Closed Systems**: Proprietary and self-contained, generally more secure but less flexible

**Security Defaults**

* **Security Defaults**: Ensures baseline security settings are in place to reduce risks of misconfiguration

**Fail Securely**

* **Concept**: Systems should fail in a secure manner to prevent unauthorized access during failures
  + **Exception Handling**: Manage errors to maintain security when unexpected events occur
  + **Fail-Safe vs. Fail-Secure**:
    - **Fail-Safe**: Prioritizes safety, minimizes harm or data exposure
    - **Fail-Secure**: Prioritizes security, limits access during failure

**Security Design Principles**

* **Keep It Simple (KISS)**: Simpler designs are easier to secure, audit, and maintain
* **Zero Trust**:
  + **Assume Breach**: "Never trust, always verify" approach
  + **Continuous Verification**: Ongoing validation of user and device access

**Privacy by Design (PbD)**

* **Privacy by Design**: Embedding privacy controls into systems and processes from the beginning

**Trust and Assurance**

* **Trust and Assurance**: Confidence in system security based on design, testing, and operational controls

**Trusted Computing Base (TCB)**

* **Trusted Computing Base**: Collection of hardware, software, and controls enforcing a system’s security policy

**Security Models**

* **Bell-LaPadula Model**: Focuses on confidentiality with "no read up, no write down"
* **Biba Model**: Focuses on integrity with "no write up, no read down"
* **Clark-Wilson Model**: Emphasizes integrity through well-formed transactions and separation of duties
* **Brewer-Nash Model (Chinese Wall)**: Prevents conflict of interest in accessing sensitive data
* **Graham-Denning Model**: Details rights and permissions for creating, transferring, and modifying subjects and objects
* **Harrison-Ruzzo-Ullman (HRU) Model**: Similar to Graham-Denning, focusing on access rights and modifications

**Computer Security Evaluation Controls**

* **ISO/IEC 15408 (Common Criteria)**: Framework for evaluating security products
  + **Protection Profiles (PP)**: Security requirements for specific product types
  + **Security Targets (ST)**: Detailed security requirements for a product under evaluation
  + **Evaluation Assurance Level (EAL)**: Levels (EAL1 to EAL7) indicating rigor of security evaluation
  + **Authorization to Operate (ATO)**: Formal permission for a system to operate in a given environment

**Security Capabilities of Information Systems**

* **Memory Protection**: Prevents processes from accessing unauthorized memory
* **Virtualization**: Creates isolated environments to enhance security and resource use
* **Trusted Platform Module (TPM)**: Hardware module for secure key storage and cryptographic functions
* **Encryption/Decryption**: Secures data in transit and at rest by encoding it
* **Interfaces**: Secure communication points for data exchange, reducing vulnerabilities
* **Fault Tolerance**: Ensures reliability and availability through redundancy and error-handling

**Information System Life Cycle**

* **Phases**: Planning, development, testing, deployment, maintenance, and decommissioning
* **Security Integration**: Incorporating security at each stage to address evolving risks and compliance needs

## Chapter 9 – Security Vulnerability, Threats, and Countermeasures

**System Responsibilities and Architecture**

* **Shared Responsibilities**: Defines security tasks shared between users, developers, and administrators
* **Protection Rings**: Layered access model for isolating privileges within a system
* **System Security Policy**: Guidelines and rules governing system behavior and access
* **Process Isolation & Hardware Segmentation**: Techniques for separating processes and securing hardware

**Memory and Storage Security**

* **Types of Memory:**
  + **ROM (Read-Only Memory):** Non-volatile memory used to store firmware; data cannot be modified easily
  + **PROM (Programmable Read-Only Memory):** A type of ROM that can be programmed once after manufacturing
  + **EPROM (Erasable Programmable Read-Only Memory):** Can be erased and reprogrammed using UV light; typically used for firmware updates
  + **UVEPROM (Ultra-Violet EPROM):** Similar to EPROM, erased using UV light, allowing reprogramming
  + **EEPROM (Electrically Erasable Programmable Read-Only Memory):** Can be electrically erased and reprogrammed multiple times; commonly used in microcontrollers and BIOS
  + **RAM (Random Access Memory):** Volatile memory used for fast data storage and retrieval while a system is running
* **Memory Addressing & Security Issues:** Vulnerabilities in accessing and protecting memory space
* **Secondary Storage Security:** Security concerns with external and removable storage devices, including unauthorized access and data loss
* **Emanation Security:** Protection against data leakage from electromagnetic emissions, which can be intercepted

**Security Risks in Input/Output and Code Execution**

* **I/O Device Risks**: Security issues posed by peripherals (e.g., USB, printers)
* **JavaScript Concerns**: Risks in client-side scripting, such as cross-site scripting (XSS)
* **Covert Channels**: Hidden data transfer methods that bypass security controls

**Modern Data Systems & Distributed Computing**

* **Large-Scale Parallel Data Systems**: Security implications of parallel processing and big data
* **Distributed Systems**: Multi-system environments with security risks in data sharing and integrity
* **Data Sovereignty**: Compliance and security issues based on the geographic location of data storage

**Specialized Technologies**

* **Operational Technology (OT) & Industrial Control Systems (ICS)**: Security needs for industrial systems
* **Internet of Things (IoT)**: Risks from interconnected smart devices
* **Embedded Systems & Microcontrollers**: Security concerns in fixed-function devices and static environments
* **Real-Time Operating Systems (RTOS)**: Specialized OS for real-time processing, with unique security challenges
* **High-Performance Computing (HPC)**: Security considerations for advanced computational environments

**Virtualization & Cloud Security**

* **Hypervisors, Virtual Software & Virtual Networking**: Key components of virtualization with unique security concerns
* **Software Defined Everything (SDx) & Virtual Desktop Infrastructure (VDI/VMI)**: Management flexibility with security trade-offs
* **Security Issues in Virtualization**: Risks in virtual machine sprawl, unauthorized access, and hypervisor vulnerabilities
* **Containerization & Kubernetes**: Security implications of containerized applications and orchestration

**Emerging Technologies**

* **Edge & Fog Computing**: Decentralized computing models that bring processing closer to the source of data with associated security risks
* **Microservices**: Security considerations in modular application development
* **Infrastructure as Code (IaC)**: Security in automated infrastructure provisioning and configuration
* **Software Defined Visibility (SDV)**: Enhancing network visibility for improved security

**Mobile Device Security**

* **Mobile Device Security & Deployment Policies**: Protecting mobile data, managing access, and enforcing security policies
* **Virtual Mobile Infrastructure (VMI)**: Virtualizing mobile environments to improve security

**Design & Coding Vulnerabilities**

* **Design and Coding Flaws**: Vulnerabilities from poor software design or insecure coding practices

## Chapter 10 – Physical Security Requirements

**Physical Security Fundamentals**

* **No Security Without Physical Security**: Physical access is foundational to securing all other forms of security

**Facility Planning and Design**

* **Security Facility Plan**: Comprehensive plan detailing physical security controls and procedures for site protection
* **Technology Convergence**: Integration of physical and digital security systems for unified management
* **Site Selection**: Choosing a secure location, considering factors like crime rates, natural disaster risks, and accessibility
* **Facility Construction Design**: Key considerations include entry points, access control zones, and structural reinforcement
* **Functional Order of Controls**: Applying physical controls in layers: deterrent, preventive, detective, and corrective controls

**Operational and Equipment Security**

* **Equipment Failure**: Planning for system resilience and availability during hardware malfunctions
* **Design and Configure Secure Work Areas**: Separate sensitive areas and apply appropriate access controls
* **Wiring Closet Security**: Protects network equipment and cabling from unauthorized access and tampering

**Access Control Devices**

* **Proximity Devices & Readers**: Cards, fobs, and biometric readers for controlling access based on proximity
* **Intrusion Detection Systems**: Monitors unauthorized access attempts and triggers alerts
* **Cameras**: Surveillance for monitoring access points and high-security areas

**Media and Evidence Storage**

* **Media Storage Security**: Protects data storage devices from unauthorized access and environmental damage
* **Evidence Storage Concerns**: Ensures secure storage and chain of custody for legal evidence

**Common Threats to Physical Security**

* **Common Threats**: Theft, vandalism, tailgating, and social engineering
* **Control Your Environment**: Manage temperature, humidity, and air quality to protect equipment

**Environmental and Fire Safety**

* **Water Leakage and Flood Management**: Protect against potential water damage from leaks, flooding, and plumbing failures
* **Fire Detection and Suppression**: Use of fire alarms, sprinklers, and gas-based suppression systems to minimize fire risk

**Perimeter and Internal Security Controls**

* **Physical Perimeter Security**: Fences, gates, lighting, and barriers to prevent unauthorized access to the facility
* **Security Guards and Guard Dogs**: Human presence and trained animals for active surveillance and deterrence
* **Visitor Management**: Procedures for handling and monitoring visitors within secure facilities
* **Internal Security Controls**: Includes locking mechanisms, secure areas, and restricted access for employees

**Performance Measurement**

* **KPIs of Physical Security**: Metrics for evaluating physical security effectiveness, such as incident response times, access control breaches, and environmental alarms

## **KGIs of Physical Security:** Metrics indicating success in achieving long-term security goals, like zero incidents or full policy compliance.

## **KRIs of Physical Security:** Metrics highlighting potential risks, such as unauthorized access attempts, equipment failures, or surveillance anomalies.

## Chapter 11 – Secure Network Architecture & Components

**Network Architecture Models**

* **OSI Model Layers**: Seven layers (Physical, Data Link, Network, Transport, Session, Presentation, Application) providing a framework for network communication
* **TCP/IP Model**: Four-layer model (Link, Internet, Transport, Application) used for internet protocols

**Network Identifiers and Addressing**

* **Network Container Names**: Names used for network segments or VLANs to isolate and manage traffic
* **MAC Addresses**: Unique hardware identifiers for devices at the Data Link layer (OSI Layer 2)
* **DNS (Domain Name System)**: Translates domain names to IP addresses
  + **DNS Poisoning**: Attack where incorrect DNS information redirects users to malicious sites
* **ARP (Address Resolution Protocol)**: Resolves IP addresses to MAC addresses for network communication

**Network Segmentation and Edge Networks**

* **Micro-Segmentation**: Divides networks into small, isolated segments for better control and security
* **Edge Networks**: Networks that operate at the boundary of the enterprise, often near end-users, such as IoT and mobile devices

**Wireless Technologies and Security**

* **Various Wireless Technologies**: Wi-Fi (802.11), Bluetooth, NFC, Zigbee
* **Site Survey**: Assessment of wireless coverage, interference, and network design needs
* **WAP (Wireless Access Point) Attacks**: Exploiting weaknesses in wireless access points
* **Captive Portals**: Pages that intercept web traffic until users authenticate or agree to terms
* **Wireless Attacks**: Includes eavesdropping, man-in-the-middle (MitM), and rogue access points

**Content Distribution and Access Control**

* **Content Delivery Networks (CDNs)**: Distributed servers that cache content closer to users to improve performance and resilience
* **Network Access Control (NAC)**: Enforces security policies on devices attempting to connect to the network

**Network Security Devices and Techniques**

* **Various Types of Firewalls**:
  + **Packet-Filtering**: Filters packets based on headers
  + **Stateful Inspection**: Tracks active connections for added context
  + **Application-Layer (Proxy) Firewall**: Inspects application-level traffic
  + **Next-Generation Firewall (NGFW)**: Includes intrusion prevention and application control
* **Proxies**: Intermediaries for web requests, providing anonymity, caching, and security filtering
* **Endpoint Security**: Protects individual devices with antivirus, EDR (Endpoint Detection and Response), and encryption

**Reports**

* **SOC 1:** Audit for financial controls impacting financial statement reliability.
* **SOC 2:** Audit for security, availability, processing, integrity, and confidentiality.
* **Type 1:** Evaluates controls' design at a specific point in time.
* **Type 2:** Evaluates controls' design and effectiveness over a defined period.

## Chapter 12 Secure Communication and Network Attacks

**Secure Communication Protocols and Authentication**

* **PPP (Point-to-Point Protocol)**: Protocol for direct communication between two network nodes, often used for dial-up and VPNs
* **PAP (Password Authentication Protocol)**: Simple, unencrypted username and password exchange (insecure)
* **CHAP (Challenge Handshake Authentication Protocol)**: Uses a challenge-response mechanism for more secure authentication
* **EAP (Extensible Authentication Protocol)**: Framework supporting various authentication methods commonly used in wireless networks
* **IEEE 802.1X**: Port-based network access control protocol commonly used for securing wired and wireless networks

**Network Access and Port Security**

* **Port Security**: Limits the devices allowed to connect to a network port, helping to prevent unauthorized access

**Voice and Remote Communication Security**

* **Voice Communication Security**: Measures to protect the confidentiality and integrity of voice transmissions, including encryption for VoIP
* **PBX Security**: Threats include unauthorized access and toll fraud; countermeasures involve strong access controls and logging
* **VoIP Security Issues**: Risks include eavesdropping and denial of service; mitigations include encryption and secure protocols
* **Phreaking**: Unauthorized tampering with telephone systems, often to make free calls

**Remote Access Security**

* **Remote Access Security Management**: Controls and policies to secure remote connections, including multi-factor authentication and VPNs
* **Remote Access Security**: Encryption, authentication, and endpoint protection to secure data during remote access

**Collaboration and Load Balancing**

* **Multimedia Collaboration Security**: Protecting shared multimedia channels (e.g., video conferencing) from eavesdropping and unauthorized access
* **Load Balancers**: Distribute network traffic across multiple servers for improved availability and redundancy
  + **Active/Active**: All servers handle traffic, enhancing load distribution and fault tolerance
  + **Active/Passive**: One server is active while others are on standby for failover

**Virtual Networks and Tunneling**

* **Virtualized Networks**: Logical networks created within physical networks, enhancing flexibility and isolation
* **Tunneling**: Encapsulating network traffic within another protocol for secure transmission
* **VPN (Virtual Private Network)**: Secures data transmission over untrusted networks through encryption
  + **Split Tunneling**: Only specific traffic is routed through the VPN, allowing direct access to other resources
  + **Full Tunneling**: All traffic is routed through the VPN, providing comprehensive security

**Network Address Translation and Connectivity**

* **NAT (Network Address Translation)**: Modifies IP address information in packet headers to facilitate private-to-public IP communication
* **Third-Party Connectivity**: Securely connecting with external networks, often requiring strict access controls and monitoring

**Communication Switching Methods**

* **Packet Switching**: Data is broken into packets and routed individually; efficient and used in IP networks
* **Circuit Switching**: Dedicated communication path for the duration of a session; used in traditional telephony

**Network Attacks and Countermeasures**

* **Network Attacks**: Includes DDoS, eavesdropping, man-in-the-middle, replay, and session hijacking
  + **Countermeasures**: Encryption, firewalls, intrusion detection/prevention systems (IDPS), strong authentication, and monitoring

## Chapter 13 – Managing Identity and Authentication

**Access Control Types**

* **Physical Access Controls**: Protect physical assets with barriers like locks, badges, and biometrics
* **Logical Access Controls**: Protect digital assets through mechanisms like passwords, permissions, and encryption

**Identity Management Concepts**

* **Subject vs. Object**:
  + **Subject**: Entity (user, process) requesting access
  + **Object**: Resource or asset being accessed
* **AAA Model (Authentication, Authorization, Accounting)**: Ensures proper user verification, access rights, and activity logging

**Identification vs. Authentication**

* **Identification**: User declares their identity (e.g., username)
* **Authentication**: Verification of declared identity (e.g., password, biometrics)
* **Establishment of Identity, Registration, and Proofing**: Processes to verify and record user identity for access control

**Authorization and Accounting**

* **Authorization**: Determines user permissions after successful authentication
* **Accounting**: Logs and monitors user actions to maintain records of access

**Authentication Factors**

* **Primary Authentication Factors**:
  + **Something You Know** (e.g., password)
  + **Something You Have** (e.g., token)
  + **Something You Are** (e.g., biometrics)
* **Important Authentication Concepts**: Multi-factor authentication (MFA), adaptive authentication, risk-based authentication

**Identity Systems and Management**

* **Single Sign-On (SSO)**: Allows users to authenticate once and access multiple systems seamlessly
* **Federated Identity Systems**: Enables cross-domain authentication using trusted third-party identity providers
* **Just-In-Time (JIT) Provisioning**: Creates user accounts dynamically at the time of access

**Credential and Session Management**

* **Credential Management Systems**: Secure storage, issuance, and revocation of credentials
* **Session Management**: Controls the duration and security of user sessions to prevent unauthorized reuse

**Identity and Access Life Cycle**

* **Provisioning Life Cycle**: Includes onboarding, managing, and de-provisioning access for users
* **Group and Role Definition**: Organizes users by roles and groups to simplify access management
* **Account Access Reviews**: Regular audits of user access to ensure adherence to least privilege and remove stale accounts

## Chapter 14 – Controlling and Monitoring Access

**Authorization Mechanisms**

* **Common Authorization Mechanisms**: Methods to control user access to resources, including permissions, roles, and policies

**Access Control Models**

* **Discretionary Access Control (DAC)**: Access rights are managed by the resource owner, allowing flexibility but potentially less security
* **Role-Based Access Control (RBAC)**: Access is granted based on user roles, simplifying permissions management by grouping users with similar access needs
* **Rule-Based Access Control**: Uses rules to determine access, often applied in firewall and network access configurations
* **Attribute-Based Access Control (ABAC)**: Access decisions are based on multiple attributes, such as user role, time, location, and device type
* **Mandatory Access Control (MAC)**: Access is controlled by a central authority based on classifications, enforcing strict policies for sensitive data
* **Risk-Based Access Control**: Adjusts access permissions dynamically based on real-time risk assessments

**Sign-On Methods and Protocols**

* **Sign-On Methods on the Internet**: Includes Single Sign-On (SSO), social media logins, and federated identity management
* **Kerberos**: Network authentication protocol using tickets and time-stamped authentication to prevent replay attacks
* **AAA Protocols (Authentication, Authorization, Accounting)**: Framework for controlling and monitoring user access and logging activity

**Access Risks and Attacks**

* **Privilege Escalation**: Exploiting vulnerabilities to gain higher access privileges than initially granted
* **Zero-Trust Principles**: "Never trust, always verify"; continuous monitoring and verification of users and devices
* **Kerberos Exploitation Attacks**: Attacks on Kerberos can include ticket forging or abuse of expired tickets to gain unauthorized access

**Password Attacks**

* **Brute-Force Attacks**: Systematically tries all possible password combinations until the correct one is found
* **Dictionary Attacks**: Attempts to crack passwords using a list of common words and phrases

## Chapter 15 – Security Assessment & Testing

**Security Assessment and Testing Programs**

* **Importance**: Essential for identifying vulnerabilities, validating controls, and ensuring ongoing security posture

**Vulnerability Assessments and Penetration Tests**

* **Vulnerability Assessment**: Identifies known vulnerabilities in systems, applications, and networks
* **Penetration Testing**: Simulates real-world attacks to exploit vulnerabilities and test defense mechanisms

**Software Testing**

* **Code Validation**: Ensures that code is free of security flaws before deployment
* **Static Testing**: Analyzes code without executing it, focusing on code structure and potential flaws
* **Dynamic Testing**: Tests code during execution to identify runtime vulnerabilities
* **Peer Review**: Process to formally or informally have code reviewed

**Fuzzing**

* **Concept**: Automated testing technique that inputs random data to applications to uncover potential security flaws

**Security Management Oversight**

* **Management Tasks**: Activities that provide oversight, set policies, and ensure alignment with the organization’s security goals

**Audits and Compliance**

* **Internal, External, and Third-Party Audits**: Independent reviews of security practices to ensure compliance and identify weaknesses

**Data Collection and Analysis**

* **Collect Logs and Security Data**: Gathering log files and security metrics to monitor, detect, and respond to incidents

**Cybersecurity Exercises**

* **Cybersecurity Exercises**: Simulated incidents and tabletop exercises to prepare teams for real security threats

## Chapter 16 – Managing Security Operations

**Access Control Principles**

* **Need-to-Know vs. Least Privilege**:
  + **Need-to-Know**: Access is granted only to information necessary for a specific task
  + **Least Privilege**: Users are given the minimum level of access required to perform their role

**Operational Controls**

* **Segregation of Duties**: Divides tasks among multiple people to reduce the risk of fraud or error
* **Job Rotation**: Regularly shifts roles among employees to prevent dependency on a single individual and expose security risks
* **Monitoring Privileged Operations**: Continuous oversight of high-privilege accounts to detect and prevent misuse

**Service Agreements and Personnel Security**

* **Service-Level Agreements (SLAs)**: Formal agreements that define service expectations, performance metrics, and penalties for non-compliance
* **Personnel Safety and Security Concerns**: Protecting the physical safety of employees and ensuring secure handling of sensitive information

**Provisioning and Media Protection**

* **Secure Provisioning**: Ensuring secure setup, configuration, and deployment of systems and services
* **Media Management and Protection**: Securely handling, storing, and disposing of data storage media to prevent unauthorized access

**Cloud Service Models**

* **SaaS (Software as a Service)**: Cloud-based applications accessible over the internet
* **PaaS (Platform as a Service)**: Provides a platform for developing, testing, and deploying applications
* **IaaS (Infrastructure as a Service)**: Offers virtualized computing resources over the internet
* **Serverless Architecture**: Allows developers to build applications without managing server infrastructure

**Cloud Security Management**

* **Managed Services in the Cloud**: Security considerations for third-party cloud services, including data control, compliance, and vendor security practices

**Configuration and Change Management**

* **Configuration and Change Control Management**: Processes to ensure that system changes are planned, documented, and authorized
* **Patch Management**: Regularly updating software to fix security vulnerabilities and improve functionality

**Vulnerability Management**

* **Vulnerability Management**: Identifying, assessing, and remediating security weaknesses in systems

## Chapter 17 – Preventing and Responding to Incidents

**Incident Management and Prevention**

* **Incident Management Steps**: Identification, containment, eradication, recovery, and lessons learned
* **Basic Prevention Measures**: Strong access controls, regular updates, network segmentation, and employee training

**Access Control Techniques**

* **Whitelisting vs. Blacklisting**:
  + **Whitelisting**: Allows only approved applications or IPs
  + **Blacklisting**: Blocks specific applications or IPs known to be malicious
* **Sandboxing**: Isolates applications or files in a secure environment to prevent harm to the main system

**Third-Party Security Services**

* **Third-Party Security Services**: External providers for services such as managed detection and response, vulnerability assessments, and firewall management

**Common Attack Types**

* **Denial-of-Service (DoS) Attacks**: Overloading a network or system to disrupt service
* **Zero-Day Exploits**: Attacks on unknown vulnerabilities before patches are available
* **Man-in-the-Middle (MitM) Attacks**: Intercepting and potentially altering communications between two parties

**Intrusion Detection and Prevention**

* **Intrusion Detection Systems (IDS)**: Monitors for suspicious activity and alerts on potential threats
* **Intrusion Prevention Systems (IPS)**: Detects and actively blocks malicious traffic

**Deceptive Security Techniques**

* **Honeypots**: Decoy systems set up to attract and analyze attacker behavior
* **Honeynets**: Networks of honeypots designed to capture detailed information on intrusion tactics

**Malware Blocking and Monitoring**

* **Methods to Block Malicious Code**: Antivirus, application whitelisting, firewalls, and email filtering
* **Types of Log Files**: Security logs, application logs, system logs, and audit logs for monitoring and forensic analysis

**Monitoring and Accountability**

* **Monitoring Tools**: Tools like SIEM (Security Information and Event Management), IDS/IPS, and network monitoring to track and respond to threats
* **Audit Trails**: Detailed records of user and system activity to trace actions and maintain accountability

**Threat Intelligence and Response Automation**

* **Threat Feeds**: Regular updates on emerging threats from external sources
* **Threat Hunting**: Proactively searching for threats in the environment that may have evaded defenses
* **SOAR (Security Orchestration, Automation, and Response)**: Automates security responses, improves incident management efficiency, and integrates multiple security tools

## Chapter 18 – Disaster Recovery Planning

**Types of Disasters**

* **Natural Disasters**: Include storms, pandemics, tsunamis, volcanic eruptions, earthquakes, floods, hurricanes, tornadoes, and wildfires; can cause significant operational disruption and data loss
* **Human-made Disasters**: Include labor disputes, infrastructure failures, cyber-attacks, terrorist acts, fires, hazardous material spills, explosions, and power outages

**Recovery Facilities**

* **Types of Recovery Facilities**:
  + **Hot Site**: Fully equipped, ready-to-use facility; minimal downtime but high cost
  + **Warm Site**: Partially equipped facility; moderate setup time and cost
  + **Cold Site**: Basic infrastructure only; lower cost but significant setup time
  + **Mobile Site**: Portable facility that can be moved to a specific location
  + **Reciprocal Agreement**: Agreement between organizations to provide facilities to each other in case of a disaster
  + **Cloud-Based Recovery**: Leveraging cloud infrastructure for flexible and scalable disaster recovery

**Mutual Assistance Agreements (MAAs)**

* **Benefits of MAAs**: Cost-effective option for disaster recovery by sharing resources between organizations
* **Common Implementation Reasons**: Useful for smaller organizations with limited budgets, but can be less reliable due to resource availability issues during widespread disasters

**Technologies for Database Backup**

* **Database Backup Technologies**: Include full backups, incremental backups, electronic vaulting, differential backups, and continuous replication technologies

**Disaster Recovery Processes**

* **Common Processes**:
  + **Risk Assessment**: Identifying potential disaster scenarios and impact
  + **Business Impact Analysis (BIA)**: Determining the operational and financial effects of disasters
  + **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**: Define acceptable downtime and data loss
  + **Data Backup**: Regular backups to ensure data availability post-disaster
  + **Communication Plan**: Procedures for internal and external communication during a disaster
  + **Training and Awareness**: Regular employee training on disaster response procedures

**Disaster Recovery Plan Testing**

* **Types of Tests**:
  + **Read-Through**: Team members review the DR plan for accuracy and completeness; minimal business disruption
  + **Tabletop Exercise**: Discussion-based simulation of a disaster scenario; minimal impact on operations
  + **Walk-Through Drill**: Teams perform a step-by-step review of the DR plan; low impact
  + **Simulation Test**: Simulates a disaster scenario without affecting actual systems; moderate impact
  + **Parallel Test**: DR systems are activated to verify functionality without disrupting production; moderate impact
  + **Full-Interruption Test**: Entire organization operates from the DR site; highest impact and risk but most comprehensive

## Chapter 19 – Investigations and Ethics

**Computer Crime**

* **Definition**: Illegal activities involving computers or networks, including hacking, fraud, and cyber espionage
* **Categories of Computer Crime**:
  1. **Computer as a Target**: Attacks like DDoS or hacking
  2. **Computer as a Tool**: Crimes facilitated by computers, such as fraud
  3. **Computer as Incidental**: Crimes where computers play a minor role, e.g., storing stolen data
  4. **Computer as a Symbol**: Cyber vandalism or defamation against organizations
  5. **Personal Crimes**: Cyberstalking, harassment, or identity theft
  6. **Property Crimes**: Intellectual property theft, piracy, or unauthorized access

**Evidence Collection and Discovery**

* **Importance of Collecting Evidence**: Proper evidence collection is crucial for supporting legal actions and investigations
* **Discovery Process**: Pre-trial phase where parties exchange information and evidence

**Intrusion Investigation**

* **Investigating Intrusions**: Identify and analyze artifacts from systems, software, and data to understand the scope and method of an intrusion

**Confiscating Evidence**

* **Alternatives for Evidence Confiscation**:
  + **Seizure**: Physically taking the equipment for analysis
  + **Duplication**: Creating forensic copies without removing original equipment
  + **Remote Collection**: Collecting data remotely when physical access is impractical
  + **Appropriate Use**: Based on sensitivity, legality, and practicality of each case

**Retention and Admissibility of Evidence**

* **Retention of Investigatory Data**: Maintains the integrity of data and allows for historical analysis
* **Requirements for Evidence to Be Admissible**:
  + **Relevance**: Evidence must relate directly to the case
  + **Reliability**: Collected in a way that maintains integrity
  + **Legality**: Obtained lawfully to be admissible in court

**Types of Evidence**

* **Various Types of Evidence**:
  + **Direct Evidence**: Witness testimony or video of the crime
  + **Circumstantial Evidence**: Indirect evidence suggesting involvement
  + **Corroborative Evidence**: Supports or confirms other evidence
  + **Digital Evidence**: Emails, logs, or files from computers and networks

**Ethics in Security**

* **Importance of Ethics to Security Personnel**: Upholds trust, integrity, and responsibility in security practices
* **(ISC)² Code of Ethics and RFC 1087**:
  + **(ISC)² Code**: Guidelines for conduct, integrity, and respect for the public and profession
  + **RFC 1087**: Ethical use of the internet, prohibiting malicious activities and upholding the internet as a public resource

## Chapter 20 – Software Development Security

**Database Architecture**

* **Relational Database Management System (RDBMS)**: Organizes data into tables with rows and columns, supporting relationships between data entities and enabling SQL-based querying

**Intelligent Systems**

* **Expert Systems**: AI systems that use rules and data to make decisions, often emulating human expertise
* **Machine Learning**: Algorithms that learn from data to make predictions or decisions without explicit programming
* **Neural Networks**: Machine learning models inspired by the human brain, often used in deep learning applications

**System Development Models**

* **Models of System Development**: Include Waterfall, V-Model, Spiral, and Agile, each with unique approaches to project phases and iterations

**Agile and Scrum**

* **Scrum Approach**: A framework within Agile methodology emphasizing iterative development, daily stand-ups, and sprint-based progress. Integrated product teams (IPT) are an early effort at this approach.

**Software Development Maturity Models**

* **Maturity Models**: Frameworks (e.g., Capability Maturity Model Integration - CMMI) that assess the development process’s maturity, from ad hoc practices to optimized processes

**SW-CMM (Software Capability Maturity Model):**

* **Purpose**: Assesses the maturity of software development processes, from ad hoc to optimized.
* **Levels:**
  1. **Initial:** Unpredictable processes
  2. **Repeatable:** Basic project management in place
  3. **Defined:** Standardized, documented processes
  4. **Managed:** Quantitative process measurement
  5. **Optimizing:** Continuous improvement focus

**IDEAL Model:**

* **Purpose:** Guides organizations through structured process improvement.

**Phases:**

* 1. **Initiating:** Define goals and gain support
  2. **Diagnosing:** Assess current state
  3. **Establishing:** Plan improvements
  4. **Acting:** Implement changes
  5. **Learning:** Review and refine practices

**SAMM (Software Assurance Maturity Model):**

* **Purpose:** Framework by OWASP for improving software security practices.
* **Structure:** Five domains—Governance, Design, Implementation, Verification, and Operations—each with progressive maturity levels to enhance secure development practices.

**Change and Configuration Management**

* **Importance of Change and Configuration Management**: Ensures all changes are documented, authorized, and traceable, reducing the risk of unauthorized modifications and maintaining system stability

**Testing in Software Development**

* **Importance of Testing**: Validates functionality, performance, and security, helping to identify bugs and vulnerabilities before deployment

**Coding Tools in Development**

* **Role of Coding Tools**: Integrated Development Environments (IDEs), version control (e.g., Git), and code analyzers assist in writing, managing, and optimizing code

**Acquired Software and Organizational Impact**

* **Impact of Acquired Software**: Brings potential risks, including compatibility issues, security vulnerabilities, and the need for vendor support

## Chapter 21 – Malicious Code and Application Attacks

**Malicious Code Propagation and Threats**

* **Virus Propagation Techniques**: Viruses spread through **infected file injection, boot sector infection, macro infection, and service infection**, aiming to replicate and infect systems
* **Ransomware Threats**: Malicious software that encrypts files or systems, demanding payment for decryption; disrupts operations and can lead to data loss

**Antivirus Detection**

* **How Antivirus Detects Viruses**: Uses signature-based detection for known malware, heuristic analysis for suspicious behavior, and sometimes AI to identify new threats

**User and Entity Behavior Analytics (UEBA)**

* **UEBA Functions**: Monitors and analyzes user and device behaviors to detect anomalies that could indicate insider threats or compromised accounts

**Application Attacks**

* **Types of Application Attacks**: Include SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), buffer overflow, and denial of service (DoS), exploiting weak code or configurations

**Web Application Vulnerabilities and Countermeasures**

* **Two Common Vulnerabilities**:
  + **Injection Flaws**: Prevented by input validation and parameterized queries
  + **Broken Authentication**: Secured with strong session management and multi-factor authentication
  + **Sensitive Data Exposure**: Mitigated with encryption and secure data storage practices
  + **Security Misconfiguration**: Addressed by regular security assessments and adhering to secure coding practices

**Cross-Site Scripting (XSS)**

* **Overview**: XSS allows attackers to inject malicious scripts into web pages, running them in users' browsers to steal data, hijack sessions, or alter page content.
* **Types**:
  + **Stored**: Script is saved on the server and served to multiple users.
  + **Reflected**: Script is reflected via URL parameters.
  + **DOM-Based**: Script injection occurs in the client’s browser.
* **Countermeasures**: Input validation, output encoding, HTTPOnly cookies, and implementing Content Security Policy (CSP).

**SQL Injection (SQLi)**

* **Overview**: SQLi lets attackers manipulate SQL queries to bypass authentication, access or alter data, and even control databases.
* **Mechanism**: Exploits improperly sanitized user inputs in SQL queries (e.g., injecting ' OR '1'='1).
* **Countermeasures**: Use parameterized queries, stored procedures, input validation, and least privilege access.